Data Breach and Cyber Liability

John Speer
Bass Berry & Sims (Memphis, TN)

901.543.5919 | jspeer@bassberry.com
http://www.bassberry.com/jspeer/

Red Flags Rule

finra.org

On January 1, 2011, the Federal Trade Commission (FTC) began enforcing its Fair and Accurate Credit Transactions Act of 2003 (FACT Act) Red Flags Rule. The Red Flags Rule requires that each "financial institution" or "creditor"—which includes most securities firms—implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of "covered accounts." These include consumer accounts that permit multiple payments or transactions, such as a retail brokerage account, credit card account, margin account, checking or savings account, or any other accounts with a reasonably foreseeable risk to customers or your firm from identity theft.

On July 21, 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) transferred responsibility for rulemaking and enforcement of identity theft red flag rules and guidelines to the SEC and CFTC for the firms they regulate.

On Feb. 28, 2012, the SEC and CFTC jointly proposed for comment identity theft red flag rules and guidelines that are substantially similar to the FTC Red Flags Rule and do not propose new requirements or cover new entities. The proposed rules and guidelines do, however, include examples and minor language changes to help securities and commodities firms comply. The comment period closed May 7, 2012.

Customer Information Protection

finra.org

Below is information about firms' obligations to protect customer account information and links to resources to help firms meet those obligations.

See also: Firm Identity Protection

Protection of financial and personal customer information is a key responsibility and obligation of FINRA member firms. Under the SEC's Regulation S-P, firms are required to have policies and procedures addressing the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information and against unauthorized access to or use of customer records or information.

Firms should be aware that customer information and records can be compromised in a variety of ways. This is especially true for firms that offer online, Web-based access to trading platforms. Firms must understand and address the potential risks of brokerage account intrusions, whereby an unauthorized person gains access to a customer account and either steals available assets or misuses the account to manipulate the market. Intrusions are generally accomplished through the theft of the login credentials of a customer or firm employee.

Since this type of illicit activity can raise both investor protection and market integrity concerns, it is essential that firms use reasonable measures to protect customer information and assets.

Firm Checklist for Compromised Accounts

What should a firm do after it discovers that a customer's account has been compromised?

Below is a checklist of some steps that a firm may need to take if it learns that an unauthorized person may have gained entry to a customer's brokerage account. This checklist is not exhaustive, and a firm may need to take other steps depending on the nature or cause

of the intrusion, the firm's business model, the firm's customer base, shifting security threats, and changes in law.

Monitor, limit, or temporarily suspend activity in the account until the situation is resolved.

Alert others in the firm (including the firm's Legal and Compliance Department, if applicable) to be mindful of unusual activity in other customer accounts. Firms may want to consider designating in advance a specific individual or department to serve as a central contact for questions about account intrusion.

Identify, if possible, the root cause of the account intrusion (e.g., the firm's system was compromised, the individual account was hacked, the customer was the victim of identity theft) and determine whether the intrusion is isolated to one account.

If the firm is not self-clearing, notify its clearing firm of the situation.

Contact the SEC and your FINRA Coordinator. In the event of an account intrusion, have the following information readily available if possible:

- Firm information (both the introducing and clearing firms involved)
    - Firm name and CRD number
    - Firm contact name and telephone number
- Date(s) and time(s) of activity
- IP addresses used to access the account
- Security or securities involved (name and symbol)
- Time and date of the activity
- Details of the trades or unexecuted orders
- Details concerning any wire transfer activity
- Customer account affected by the activity, including name and account number
- Whether the customer has been or will be reimbursed and by whom

If appropriate, contact law enforcement agencies, such as the FBI or, if the U.S. mail is involved, the United States Postal Inspector.

Contact the firm's relevant state regulatory authorities.

If the firm has not already done so, contact the customer and, if appropriate, change the password and/or account number. For more information, view ways a firm can help a customer that has been the victim of identity theft.

Determine whether any unauthorized person has gained access to an account holder's personally identifiable information and, if so, whether the firm must provide a specific type of notification to the customer or others under state law regarding the loss of the customer's information. Some states require notice to the Attorney General or other state law enforcement agencies if a customer's "personally identifiable financial information" has been compromised.

Determine whether the firm should file a Suspicious Activity Report (SAR) under the federal anti-money laundering provisions.

FEDERAL REGISTER

Vol. 78 Friday,
No. 76 April 19, 2013

Part II

Commodity Futures Trading Commission

7 CFR Part 162

Securities and Exchange Commission

17 CFR Part 248

Identity Theft Red Flags Rules; Final Rule

COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 162

RIN 3038–AD14

SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 248

[Release Nos. 34–69359, IA–3582, IC–30456; File No. S7–02–12]

RIN 3235–AL26

Identity Theft Red Flags Rules

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

ACTION: Joint final rules and guidelines.

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

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

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

SUPPLEMENTARY INFORMATION: The Commissions are adopting new rules and guidelines on identity theft red flags for entities subject to their respective enforcement authorities. The CFTC is adding new subpart C ("Identity Theft Red Flags") to part 162 of the CFTC's regulations [17 CFR part 162] and the SEC is adding 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 [15 U.S.C. 1681–1681x], the Commodity Exchange Act [7 U.S.C. 1–27f], the Securities Exchange Act of 1934 [15 U.S.C. 78a–78pp], 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

The growth and expansion of information technology and electronic communication have made it increasingly easy to collect, maintain, and transfer personal information about individuals.[1] Advancements in technology also have led to increasing threats to the integrity and privacy of personal information.[2] 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.[3]

The Fair Credit Reporting Act of 1970 ("FCRA"),[4] as amended in 2003,[5] required several federal agencies to issue joint rules and guidelines regarding the detection, prevention, and mitigation of identity theft for entities that are subject to their respective enforcement authorities (also known as

[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] A recent survey found that in 2012, over 5% of Americans were victims of identity fraud. *See* Javelin Strategy & Research, 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters (Feb. 2013), *available at https://www.javelinstrategy.com/uploads/web_brochure/1303.R_2013IdentityFraudBrochure.pdf; see also* Comment Letter of Tyler Krulla ("Tyler Krulla Comment Letter") (Apr. 27, 2012) ("In today's technology driven world it is easier than ever for anyone to acquire and exploit someone's identity and cause severe financial problems.").

[3] *See, e.g.,* Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), *available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf* (a White House proposal to establish a consumer privacy bill of rights); The President's Identity Theft Task Force Report (Sept. 2008), *available at http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf;* Securities and Exchange Commission, Online Brokerage Accounts: What you can do to Safeguard Your Money and Your Personal Information, *available at http://www.sec.gov/investor/pubs/onlinebrokerage.htm.*

[4] Pub. L. 91–508, 84 Stat. 1114 (1970), *codified at* 15 U.S.C. 1681–1681x.

[5] *See* Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108–159, 117 Stat. 1952 (2003) ("FACT Act").

the ''identity theft red flags rules'').[6] Those agencies were the Office of the Comptroller of the Currency (''OCC''), the Board of Governors of the Federal Reserve System (''Federal Reserve Board''), the Federal Deposit Insurance Corporation (''FDIC''), the Office of Thrift Supervision (''OTS''), the National Credit Union Administration (''NCUA''), and the Federal Trade Commission (''FTC'') (together, the ''Agencies'').[7] In 2007, the Agencies issued joint final identity theft red flags rules.[8] At the time the Agencies adopted their rules, the FCRA did not require or authorize the CFTC and SEC to issue identity theft red flags rules. Instead, the Agencies' rules applied to entities that registered with the CFTC and SEC, such as futures commission merchants, broker-dealers, investment companies, and investment advisers.[9]

In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (''Dodd-Frank Act'') [10] amended the FCRA to add the CFTC and SEC to the list of federal agencies that must jointly adopt and individually enforce identity theft red flags rules.[11] 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 subject to each agency's enforcement authority. In February 2012, the Commissions jointly proposed for public notice and comment identity theft red flags rules and guidelines and card issuer rules.[12]

The CFTC and SEC received a total of 27 comment letters on the proposal.[13] Most commenters generally supported the proposal, and many stated that the rules would benefit individuals.[14] Commenters expressed concern about the prevalence of identity theft and supported our efforts to reduce it.[15] Commenters also supported the Commissions' proposal to adopt rules that would be substantially similar to the rules the Agencies adopted in 2007.[16] Some commenters raised questions about the scope of the proposal and the meaning of certain definitions.[17] One commenter stated that benefits to consumers would outweigh the costs of the rules,[18] while another took issue with the estimated costs of complying with the rules.[19]

Today, the CFTC and SEC are adopting the identity theft red flags rules. The final rules are substantially similar to the rules the Commissions proposed,[20] and to the rules the Agencies adopted in 2007.[21] The final rules apply to ''financial institutions'' and ''creditors'' subject to the Commissions' respective enforcement authorities, and as discussed further below, do not exclude any entities registered with the Commissions from their scope. The Commissions recognize that entities subject to their respective enforcement authorities, whose activities fall within the scope of the rules, should already be in compliance with the Agencies' joint rules. The rules we are adopting today do not contain requirements that were not already in the Agencies' rules, nor do they expand the scope of those rules to include new categories of entities that the Agencies' rules did not already cover. The rules and this adopting release do contain examples and minor language changes designed to help guide entities within the SEC's enforcement authority in complying with the rules, which may lead some entities that had not previously complied with the Agencies' rules to determine that they fall within the scope of the rules we are adopting today.

[6] *See* FCRA sections 615(e)(1)(A)–(B), 15 U.S.C. 1681m(e)(1)(A)–(B). Section 615(e)(1)(A) of the FCRA requires the Agencies to 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) requires the Agencies to 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.''

[7] The FCRA also required the Agencies to prescribe joint rules applicable to issuers of credit and debit cards, to require that such issuers assess the validity of notifications of changes of address under certain circumstances (the ''card issuer rules''). *See* FCRA section 615(e)(1)(C), 15 U.S.C. 1681m(e)(1)(C).

[8] *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 rules included card issuer rules. *See supra* note 7. The OCC, Federal Reserve Board, FDIC, OTS, and NCUA began enforcing their identity theft red flags rules on November 1, 2008. The FTC began enforcing its identity theft red flags rules on January 1, 2011.

[9] *See* 2007 Adopting Release, *supra* note 8.

[10] 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.*

[11] *See* FCRA section 615(e)(1), 15 U.S.C. 1681m(e)(1). In addition, section 1088(a)(10)(A) 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 24. 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).

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

[13] Comments on the proposal, including comments referenced in this release, are available on the SEC's Web site at *http://www.sec.gov/comments/s7-02-12/s70212.shtml* and the CFTC's Web site at *http://comments.cftc.gov/PublicComments/CommentList.aspx?id=1171.*

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

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

[16] *See, e.g.,* Comment Letter of the Investment Company Institute (May 1, 2012) (''ICI Comment Letter'').

[17] *See, e.g.,* Comment Letter of the Investment Adviser Association (May 7, 2012) (''IAA Comment Letter'') (requesting that the SEC and CFTC clarify the definitions of ''financial institution'' and ''creditor'' and exclude investment advisers from the categories of entities specifically mentioned in the scope section of the rule); Comment Letter of the Options Clearing Corporation (May 3, 2012) (''OCC Comment Letter'') (requesting that the SEC and CFTC clarify the definition of ''creditor'' and expressly exclude clearing organizations from the scope section of the rule); Comment Letter of the Financial Services Roundtable and the Securities Industry and Financial Markets Association (May 2, 2012) (''FSR/SIFMA Comment Letter'') (requesting that the SEC specifically exclude certain categories of entities from the definitions of ''financial institution'' and ''covered account,'' and that the SEC and CFTC specifically define the types of accounts that would qualify as covered accounts).

[18] *See* Erik Speicher Comment Letter.

[19] *See* FSR/SIFMA Comment Letter. We discuss estimated costs and benefits in the Section III of this release.

[20] *See infra* Section II.A.1.ii (discussing a revision to proposed definition of ''creditor''); *see also* § 248.201(b)(2)(i) (SEC) (revising the term ''non U.S. based financial institution or creditor,'' which was included in the proposed definition of ''board of directors,'' to ''foreign financial institution or creditor,'' for clarity and consistency with the CFTC's and Agencies' respective identity theft red flags rules).

[21] *See* 2007 Adopting Release.

II. Explanation of the Final Rules and Guidelines

A. Final Identity Theft Red Flags Rules

Sections 615(e)(1)(A) and (B) of the FCRA, as amended by the Dodd-Frank Act, require that the Commissions jointly establish and maintain guidelines for ''financial institutions'' and ''creditors'' regarding identity theft, and adopt rules requiring such institutions and creditors to establish reasonable policies and procedures for the implementation of those guidelines.[22] Under the final rules, a financial institution or creditor that offers or maintains ''covered accounts'' must establish an identity theft red flags program designed to detect, prevent, and mitigate identity theft. To that end, the final rules discussed below specify: (1) Which financial institutions and creditors must develop and implement a written identity theft prevention program (''Program''); (2) the objectives of the Program; (3) the elements that the Program must contain; and (4) the steps financial institutions and creditors need to take to administer the Program.

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

The ''scope'' subsections of the rules generally set forth the types of entities that are subject to the Commissions' identity theft red flags rules.[23] Under these subsections, the rules apply to entities over which Congress recently granted the Commissions enforcement authority under the FCRA.[24] The Commissions' scope provisions are similar to those contained in the rules adopted by the Agencies, which limit the rules' scope to entities that are within the Agencies' respective enforcement authorities.[25]

As noted above, the CFTC's ''scope'' subsection ''applies to financial institutions and creditors that are subject to'' the CFTC's enforcement authority under the FCRA.[26] The CFTC's proposed definitions of ''financial institution'' and ''creditor'' describe the entities to which its identity theft red flags rules and guidelines apply. In the Proposing Release, the CFTC defined ''financial institution'' as having the same meaning as in section 603(t) of the FCRA.[27] In addition, the CFTC's proposed definition of ''financial institution'' also specified that the term includes any futures commission merchant (''FCM''), retail foreign exchange dealer (''RFED''), commodity trading advisor (''CTA''), commodity pool operator (''CPO''), introducing broker (''IB''), swap dealer (''SD''), or major swap participant (''MSP'') that directly or indirectly holds a transaction account belonging to a consumer.[28] Similarly, in the CFTC's proposed definition of ''creditor,'' the CFTC applies the definition of ''creditor'' from 15 U.S.C. 1681m(e)(4) to any FCM, RFED, CTA, CPO, IB, SD, or MSP that ''regularly extends, 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.'' [29] The CFTC has determined that the final identity theft red flags rules apply to these entities because of the increased likelihood that these entities open or maintain covered accounts, or pose a reasonably foreseeable risk to customers, or to the safety and soundness of the financial institution or creditor, from identity theft. This approach is consistent with the general scope of part 162 of the CFTC's regulations.[30]

One commenter suggested that the CFTC follow the SEC's approach and simply cross-reference the FCRA definition of ''financial institution'' and the FCRA definition of ''creditor'' as amended by the Red Flag Program Clarification Act of 2010 (''Clarification Act'') [31] rather than including named entities in the definition.[32] The commenter argued that cross-referencing the FCRA definitions, as amended by the Clarification Act, rather than including specific types of entities that are subject to the CFTC's enforcement authority in the definitions of ''financial institution'' and ''creditor,'' would be more consistent with the SEC's and the Agencies' regulations and would allow the agencies to easily adapt to any changes to the FCRA over time.[33]

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

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

- A broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934 (''Exchange Act'');
- An investment company that is registered or required to be registered under the Investment Company Act of 1940 (''Investment Company Act''), that has elected to be regulated as a business

---

[22] 15 U.S.C. 1681m(e)(1)(A) and (B). Key terms such as ''financial institution'' and ''creditor'' are defined in the rules and discussed later in this Section.

[23] § 162.30(a) (CFTC); § 248.201(a) (SEC).

[24] 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 ''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'').

[25] *See, e.g.*, 12 CFR 334.90(a) (stating that the FDIC's red flags rule ''applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers)''); 12 CFR 717.90(a) (stating that the NCUA's red flags rule ''applies to a financial institution or creditor that is a federal credit union'').

[26] § 162.30(a); *see also supra* note 24.

[27] *See* 15 U.S.C. 1681a(t) (defining ''financial institution'' to include certain banks and credit unions, and ''any other person that, directly or indirectly, holds a transaction account (as defined in Section 19(b) of the Federal Reserve Act) belonging to a consumer''). 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 or withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third parties or others.'' 12 U.S.C. 461(b)(1)(C).)

[28] § 162.30(b)(7).

[29] § 162.30(b)(5).

[30] § 162.1(b) (specifying that ''[t]his part applies to certain consumer information held by * * * futures commission merchants, retail foreign exchange dealers, commodity trading advisors, commodity pool operators, introducing brokers, major swap participants and swap dealers.'')

[31] In December 2010, President Obama signed into law the Red Flag Program Clarification Act of 2010, which amended the definition of ''creditor'' in the FCRA for purposes of identity theft red flags rules. Red Flag Program Clarification Act of 2010, Public Law 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).

[32] IAA Comment Letter.

[33] The commenter also noted that the CFTC's proposed definition of ''creditor'' would include certain entities such as CPOs and CTAs—entities that do not extend credit.

development company ("BDC") under that Act, or that operates as an employees' securities company ("ESC") under that Act; or

• An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940 ("Investment Advisers Act").[34]

The types of entities listed by name in the scope section are the registered entities regulated by the SEC that are most likely to be financial institutions or creditors, *i.e.,* brokers or dealers ("broker-dealers"), investment companies, and investment advisers.[35] The scope section also includes any other entities that are registered or are required to register under the Exchange Act.[36] Some types of entities required to register under the Exchange Act, such as nationally recognized statistical rating organizations ("NRSROs"), self-regulatory organizations ("SROs"), municipal advisors, and municipal securities dealers, are not listed by name in the scope section because they may be less likely to qualify as financial institutions or creditors under the FCRA.[37] Nevertheless, if any entity of a type not listed qualifies as a financial institution or creditor, it is covered by the SEC's rules. The scope section does not include entities that are not themselves registered or required to register with the SEC (with the exception of certain non-registered investment companies that nonetheless are regulated by the SEC[38]), even if they register securities under the Securities Act of 1933 or the Exchange Act, or report information under the federal securities laws.[39]

The SEC received four comment letters arguing that it should specifically exclude certain entities from the scope of the rules.[40] These commenters recommended that the scope section exclude registered investment advisers,[41] clearing organizations,[42] SROs, municipal securities dealers, municipal advisors, or NRSROs.[43] The commenters argued that these entities are unlikely to be financial institutions or creditors and that, without a specific exclusion, the scope of the rules is unclear and the rules would require these entities to periodically review their operations to ensure compliance with rules that are not relevant to their businesses.[44] Another commenter recommended that the rules not list any of the types of entities subject to the rules, because such a list could confuse entities that are on the list but do not qualify as financial institutions or creditors.[45]

We appreciate these concerns, and seek to minimize potential unnecessary burdens on regulated entities. As we acknowledge above, the entities that are not listed in the rule's scope section may be less likely to qualify as financial institutions or creditors under the FCRA, *e.g.,* because they do not hold transaction accounts for consumers.[46] The Dodd-Frank Act required the SEC to adopt identity theft red flags rules with respect to persons that are "subject to the jurisdiction of the Securities and Exchange Commission."[47] Expressly excluding from certain requirements of the rules any entities that are registered with the SEC, are subject to the SEC's enforcement authority, and are covered by the scope of the rules likely would not effectively implement the purposes of the Dodd-Frank Act and the FCRA, which are described in this release. In addition, we continue to believe that specifically listing in the scope section the entities that are likely to be subject to the rules—if they qualify as financial institutions or creditors—will provide useful guidance to those entities in determining their status under the rules. Therefore, we are adopting the scope section of the rules as proposed.

i. Definition of Financial Institution

As discussed above, the Commissions' final red flags rules apply to "financial institutions" and "creditors." As in the proposed rules, the Commissions are defining the term "financial institution" in the final rules by reference to the definition of the term in section 603(t) of the FCRA.[48] That section defines a

[34] § 248.201(a).

[35] The SEC's final rules define the scope of the identity theft red flags rules, section 248.201(a), differently than Regulation S–AM, the affiliate marketing rule the SEC adopted under the 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 SEC). 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 subject to the SEC's enforcement authority. By contrast, the Dodd-Frank Act specifies that the SEC's identity theft red flags rules should apply to a "person that is subject to the jurisdiction" of the SEC. *See* Dodd-Frank Act sections 1088(a)(8), (10). Therefore, the SEC's identity theft red flags rules apply to BDCs, ESCs, and "any * * * person that is registered or required to be registered under the Securities Exchange Act of 1934," as well as to those entities within the scope of Regulation S–AM.

The scope of the SEC's final rules also differs 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. Public Law 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. *See* 15 U.S.C. 6805(a)(3)–(5).

[36] The Dodd-Frank Act defines a "person regulated by the [SEC]," for other purposes of the 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* Dodd-Frank Act section 1002(21).

[37] The SEC believes that municipal advisors and municipal securities dealers may be less likely to qualify as financial institutions because they may be less likely to maintain transaction accounts for consumers. A commenter agreed with us that municipal advisors and municipal securities dealers may be less likely to qualify as financial institutions. *See* FSR/SIFMA Comment Letter. For further discussion, see *infra* notes 43–47 and accompanying text.

[38] As noted above, the scope of the final rules covers BDCs and ESCs, which typically do not register as investment companies with the SEC but are regulated by the SEC. BDCs file with the SEC notices of reliance on the BDC provisions of the Investment Company Act and the SEC's rules thereunder. *See* Form N–54A ("Notification of Election to be Subject to Sections 55 through 65 of the Investment Company Act of 1940 Filed Pursuant to Section 54(a) of the Act") [17 CFR 274.53]. ESCs operate pursuant to individual exemptive orders issued by the SEC that govern the companies' operations. *See* Investment Company Act section 6(b) [15 U.S.C. 80a-6(b)].

[39] *See, e.g.,* 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").

[40] *See* IAA Comment Letter; Comment Letter of the National Society of Compliance Professionals, Inc. (May 4, 2012) ("NSCP Comment Letter"); OCC Comment Letter; FSR/SIFMA Comment Letter.

[41] *See, e.g.,* IAA Comment Letter ("[W]e believe a cleaner approach would be to eliminate investment advisers from the entities specifically mentioned in the scope section."); NSCP Comment Letter ("We would urge the Commission to specifically exclude investment advisers from the scope of the rule since it is our view that any adviser that is a financial institution would already be covered by FCRA."). For further discussion, *see infra* notes 55–60 and 73–76 and accompanying text.

[42] *See* OCC Comment Letter ("[W]e encourage the Commissions to expressly exclude clearing organizations from the scope of the Proposed Rules because, as explained below, clearing organizations like OCC should not be considered 'creditors' for these purposes."). For further discussion, *see infra* note 75.

[43] *See* FSR/SIFMA Comment Letter ("Specifically, we ask that the SEC exclude * * * those entities that are unlikely to be deemed financial institutions or creditors under the FCRA, such as NRSROs, SROs, municipal advisors, municipal securities dealers, and registered investment advisers.").

[44] *See, e.g.,* NSCP Comment Letter.

[45] *See* MarketCounsel Comment Letter.

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

[47] 15 U.S.C. 1681s(b)(1)(G).

[48] 15 U.S.C. 1681a(t). *See* § 162.30(b)(7) (CFTC); § 248.201(b)(7) (SEC). The Agencies also defined "financial institution," in their identity theft red flags rules, 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).").

financial institution to include certain banks and credit unions, and ''any other person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.'' [49] Section 19(b) of the Federal Reserve Act defines ''transaction account'' to include an ''account on which the * * * account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others.'' [50] Section 603(c) of the FCRA defines ''consumer'' as an individual; [51] thus, to qualify as a financial institution, an entity must hold a transaction account belonging to an individual. The following are illustrative examples of an SEC-regulated entity that could fall within the meaning of the term ''financial institution'' because it holds transaction accounts belonging to individuals: (i) A broker-dealer that offers custodial accounts; (ii) a registered investment company that enables investors to make wire transfers to other parties or that offers check-writing privileges; and (iii) an investment adviser that directly or indirectly holds transaction accounts and that is permitted to direct payments or transfers out of those accounts to third parties.[52]

A few commenters raised concerns about the SEC's statements in the Proposing Release regarding the possibility that some investment advisers could be financial institutions under certain circumstances. These commenters argued that investment advisers generally do not ''hold'' transaction accounts, thus meaning that they would *not* be financial institutions under the definition.[53] One commenter requested that we state that investment advisers who are authorized to withdraw assets from investors' accounts to pay bills, or otherwise direct payments to third parties, on behalf of investors do not ''indirectly'' hold such accounts and therefore are not financial institutions.[54]

The SEC has concluded otherwise. As described below, some investment advisers do hold transaction accounts, both directly and indirectly, and thus may qualify as financial institutions under the rules as we are adopting them. As discussed further in Section III of this release, SEC staff anticipates that the following examples of circumstances in which certain entities, particularly investment advisers, may qualify as financial institutions may lead some of these entities that had not previously complied with the Agencies' rules to now determine that they should comply with Regulation S–ID.[55]

Investment advisers who have the ability to direct transfers or payments from accounts belonging to individuals to third parties upon the individuals' instructions, or who act as agents on behalf of the individuals, are susceptible to the same types of risks of fraud as other financial institutions, and individuals who hold transaction accounts with these investment advisers bear the same types of risks of identity theft and loss of assets as consumers holding accounts with other financial institutions. If such an adviser does not have a program in place to verify investors' identities and detect identity theft red flags, another individual may deceive the adviser by posing as an investor. The red flags program of a bank or other qualified custodian [56] that maintains physical custody of an investor's assets would not adequately protect individuals holding transaction accounts with such advisers, because the adviser could give an order to withdraw assets, but at the direction of an impostor.[57] Investors who entrust their assets to registered investment advisers that directly or indirectly hold transaction accounts should receive the protections against identity theft provided by these rules.

For instance, even if an investor's assets are physically held with a qualified custodian, an adviser that has authority, by power of attorney or otherwise, to withdraw money from the investor's account and direct payments to third parties according to the investor's instructions would hold a transaction account. However, an adviser that has authority to withdraw money from an investor's account solely to deduct its own advisory fees would not hold a transaction account, because the adviser would not be making the payments to third parties.[58]

Registered investment advisers to private funds also may directly or indirectly hold transaction accounts.[59] If an individual invests money in a private fund, and the adviser to the fund has the authority, pursuant to an arrangement with the private fund or the individual, to direct such individual's investment proceeds (*e.g.*, redemptions, distributions, dividends, interest, or other proceeds related to the individual's account) to third parties, then that adviser would indirectly hold a transaction account. For example, a private fund adviser would hold a transaction account if it has the authority to direct an investor's redemption proceeds to other persons upon instructions received from the investor.[60]

ii. Definition of Creditor

The Commissions' final definitions of ''creditor'' refer to the definition of

[49] 15 U.S.C. 1681a(t). In full, the FCRA defines ''financial institution'' to mean ''a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or 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.'' *Id.*

[50] 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.'' *Id.*

[51] 15 U.S.C. 1681a(c).

[52] The CFTC's definition specifies that financial institution ''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.'' *See* § 162.30(b)(7).

[53] *See, e.g.*, IAA Comment Letter (''Investment advisers are not banks or credit unions and do not hold transaction accounts, such as custodial accounts or accounts with check-writing privileges. Instead, any cash or securities managed by investment advisers must be held in custody with financial institutions that are qualified custodians (broker-dealers or banks, primarily).'').

[54] *See* MarketCounsel Comment Letter (''MarketCounsel requests additional clarification in the Proposed Rule to make it clear that an investment adviser will not be deemed to indirectly hold a transaction account simply because it has control over, or access to, the transaction account.'').

[55] SEC staff understands, based on comment letters and communications with industry representatives, that a number of investment advisers may not currently have identity theft red flags Programs. *See* MarketCounsel Comment Letter; IAA Comment Letter. SEC staff also expects, based on Investment Adviser Registration Depository (IARD) data, that certain private fund advisers could potentially meet the definition of ''financial institution'' or ''creditor.'' *See infra* note 190.

[56] *See* 17 CFR 275.206(4)–2(d)(6) (setting forth the entities that fall within the definition of ''qualified custodian'').

[57] *See, e.g.*, Byron Acohido, *Cybercrooks fool financial advisers to steal from clients*, USA Today, Aug. 26, 2012, *available at http://usatoday30.usatoday.com/money/perfi/basics/story/2012-08-26/wire-transfer-fraud/57335540/1* (last visited March 4, 2013) (''In a new twist, cyber-robbers are using ginned-up email messages in attempts to con financial advisers into wiring cash out of their clients' online investment accounts. If the adviser falls for it, a wire transfer gets legitimately executed, and cash flows into a bank account controlled by the thieves—leaving the victim in a dispute with the financial adviser over getting made whole.'').

[58] *See supra* note 50 and accompanying text.

[59] A ''private fund'' is ''an issuer that would be an investment company, as defined in section 3 of the Investment Company Act, but for section 3(c)(1) or 3(c)(7) of that Act.'' 15 U.S.C. 80b–2(a)(29).

[60] On the other hand, an investment adviser may not hold a transaction account if the adviser has a narrowly-drafted power of attorney with an investor under which the adviser has no authority to redirect the investor's investment proceeds to third parties or others upon instructions from the investor.

''creditor'' in the FCRA as amended by the Clarification Act.[61] The FCRA now defines ''creditor,'' for purposes of the red flags rules, as a creditor as defined in the Equal Credit Opportunity Act[62] (''ECOA'') (*i.e.,* a person that regularly extends, renews or continues credit,[63] or makes those arrangements) that ''regularly and in the course of business * * * advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.''[64] 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 * * *''[65]

The CFTC's definition of ''creditor'' includes certain entities (such as FCMs and CTAs) that regularly extend, renew or continue credit or make those credit arrangements.[66] The proposed definition applies the definition of ''creditor'' from 15 U.S.C. 1681m(e)(4) to ''any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that regularly extends, 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.''[67] One commenter stated that the proposed definition was overly broad and unclear because it did not appear to include derivative clearing organizations (''DCOs'') such as the Options Clearing Corporation, while the SEC's definition could be read to include DCOs, and recommended that DCOs be explicitly excluded from the definition.[68] The commenter further requested that the Commissions specifically exclude DCOs from the scope of the Proposed Rules.

As the commenter noted, the CFTC's definition of ''creditor'' excludes DCOs because DCOs are not included on the list of entities that may qualify as creditors under the rule. Under the proposed CFTC rules, a ''creditor'' includes any FCM, RFED, CTA, CPO, IB, SD, or MSP that regularly extends, renews, or continues credit or makes credit arrangements. Unlike DCOs, the listed entities which are included in the CFTC definition of ''creditor'' engage in retail customer business and maintain retail customer accounts. These entities are included as potential creditors in the definition because they are the CFTC registrants most likely to collect personal consumer data. Moreover, this list of potential creditors is consistent with the general scope provisions of the part 162 rules, which also apply to FCMs, RFEDs, CTAs, CPOs, IBs, SDs, or MSPs.[69] Accordingly, the CFTC declines to provide a specific exclusion for DCOs from the scope of the rule.

As proposed, the SEC's definition of ''creditor'' referred to the definition of ''creditor'' under FCRA, and stated that it ''includes lenders such as brokers or dealers offering margin accounts, securities lending services, and short selling services.''[70] The SEC proposed to name these entities in the definition because they are likely to qualify as ''creditors,'' since the funds advanced in these accounts do not appear to be for ''expenses incidental to a service provided.'' One commenter, the Options Clearing Corporation, argued that the proposed definition's reference to securities lending services could be read to mean that an intermediary in securities lending transactions is a ''creditor'' under the SEC's rules, even if the entity does not meet FCRA's definition of ''creditor.''[71] The SEC intended the proposed definition of ''creditor'' to be limited to the FCRA definition, and to include relevant examples of activities that could qualify an entity as a creditor. In order to clarify this definition and avoid an inadvertently broad meaning of the term ''creditor,'' we are revising the definition to rely on FCRA's statutory definition of the term and omit the references to specific types of lending, such as margin accounts, securities lending services, and short selling services.[72]

Some commenters stated that most investment advisers would probably not qualify as creditors under the definition.[73] One commenter believed that the proposal might have implied that investment advisers were subject to a different standard than other entities under the definition of ''creditor,'' and requested that we clarify that investment advisers may, like all other entities, take advantage of the exception in the definition to advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person.[74] Our final rules do not treat investment advisers differently than any other entity under the definition of ''creditor.''[75] An investment adviser could potentially qualify as a creditor if it ''advances funds'' to an investor that are not for expenses incidental to services provided by that adviser. For example, a private

[61] *See* § 162.30(b)(5) (CFTC); § 248.201(b)(5) (SEC); *see also supra* note 31.

[62] 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).

[63] The Commissions are defining ''credit'' by reference to its definition in the FCRA. *See* § 162.30(b)(4) (CFTC); § 248.201(b)(4) (SEC). That definition refers to the definition of credit in the ECOA, which means ''the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.'' The Agencies 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).

[64] 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).

[65] FCRA section 615(e)(4)(B), 15 U.S.C. 1681m(e)(4)(B). The Clarification Act does not define the extent to which the advancement of funds for expenses would be considered ''incidental'' to services rendered by the creditor. The legislative history indicates that the Clarification Act was intended to ensure that lawyers, doctors, and other small businesses that may advance funds to pay for services such as expert witnesses, or that may bill in arrears for services provided, should not be considered creditors under the red flags rules. *See* 156 Cong. Rec. S8288–9 (daily ed. Nov. 30, 2010) (statements of Senators Thune and Dodd).

[66] *See* § 162.30(b)(5).

[67] *See* § 162.30(b)(7).

[68] OCC Comment Letter.

[69] *See* § 162.1(b).

[70] *See* proposed § 248.201(b)(5).

[71] OCC Comment Letter.

[72] *See* § 248.201(b)(5).

[73] *See, e.g.,* MarketCounsel Comment Letter; NSCP Comment Letter (''We agree with the proposal that investment advisers are not creditors for purposes of the proposal because advisers generally do not bill in arrears. We are not aware of any situation where an investment adviser would advance funds and we would note that such advisers would likely run afoul of state rules that prohibit an adviser from loaning funds or borrowing funds from a client.'').

[74] MarketCounsel Comment Letter.

[75] The definition of ''creditor'' in FCRA also authorizes the Agencies and the Commissions to include other entities in the definition of ''creditor'' if the Commissions determine that those entities offer or maintain accounts that are subject to a reasonably foreseeable risk of identity theft. 15 U.S.C. 1681m(e)(4)(C). One commenter urged the Commissions not to exercise this authority, and particularly not to include clearing organizations as creditors under the definition. *See* OCC Comment Letter (''We believe there is no reasonable basis for concluding that the securities loan clearing services offered by OCC as described above would pose a reasonably foreseeable risk of identity theft or that such services should cause OCC to be considered a 'creditor.'''). The Commissions did not propose to specifically include clearing organizations in the definition of ''creditor'' under this authority, and the final rules do not include any additional types of entities in the definition of ''creditor'' that are not already included in the statutory definition.

fund adviser that regularly and in the ordinary course of business lends money, short-term or otherwise, to permit investors to make an investment in the fund, pending the receipt or clearance of an investor's check or wire transfer, could qualify as a creditor.[76]

iii. Definition of Covered Account and Other Terms

Under the final rules, a financial institution or creditor must establish a red flags Program if it offers or maintains "covered accounts." As in the proposed rules, the Commissions are defining the term "covered account" in the final rules 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[77] or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.[78] The CFTC's definition includes a margin account as an example of a covered account.[79] The SEC's definition includes, as examples of a covered account, 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.[80]

The Commissions are defining an "account" as a "continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes."[81] The CFTC's definition specifically includes an extension of credit, such as the purchase of property or services involving a deferred payment.[82] The SEC's definition includes, as examples of accounts, "a brokerage account, a mutual fund account (*i.e.,* an account with an open-end investment company), and an investment advisory account."[83]

In the Proposing Release, the Commissions noted that "entities that adopt red flags Programs would focus their attention on 'covered accounts' for indicia of possible identity theft."[84] In response to this statement, one commenter recommended revising the definition of "covered account" such that entities adopting red flags Programs would focus particularly on protecting various types of information provided by customers, rather than focusing on particular categories of accounts.[85] The Commissions have decided not to revise the definition of "covered account" as suggested by this commenter, because the Commissions believe that by focusing the rules on the types of accounts that might pose a reasonably foreseeable risk of identity theft, financial institutions and creditors are best able to protect the information that customers provide in the course of holding these accounts. Moreover, the current definition and scope of the term "covered account" are similar to the provisions of the other Agencies' identity theft red flags rules.[86] As discussed below, the Commissions believe that the final rules' terms should be defined as the Agencies defined them in their respective final rules, where appropriate, to foster consistent regulations.[87]

Two commenters argued that insurance company separate accounts are unlikely to be covered accounts because they are not established for personal, family, or household purposes and do not pose a reasonably foreseeable risk of identity theft.[88] They contended that insurance company separate accounts are investment vehicles underlying variable life and annuity insurance products, and generally individual customers do not have a direct relationship with these accounts. One of the commenters requested that the definition of "covered account" specifically exclude insurance company separate accounts.[89] The commenter noted that because third parties and customers do not have direct access to insurance company separate accounts, there is little risk of identity theft in these accounts.[90]

The final rules require all financial institutions and creditors to assess whether they offer or maintain covered accounts. Although, as discussed above, some commenters suggested that insurance company separate accounts may not qualify as covered accounts under the definition, the final rule does not exclude insurance company separate accounts from the definition of "covered account" because it would be impracticable to provide an exhaustive list of account types that are not covered accounts. Similarly, one commenter requested that the SEC list all of the types of accounts that would be "covered accounts" under the rules.[91] The rules provide examples of covered accounts, but we cannot anticipate all of the types of accounts that could be covered accounts. Any list that attempts to encompass all types of covered accounts would likely be under-inclusive and would not take into account future business practices.[92] The

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

[77] To be a financial institution, an entity must hold a transaction account with at least one "consumer" (defined as an "individual" in 15 U.S.C. 1681a(c)). However, once an entity is a financial institution, it must periodically determine whether it offers or maintains "covered accounts" to or on behalf of its customers, which may be individuals or business entities. Sections 162.30(b)(6) (CFTC) and 248.201(b)(6) (SEC) define "customer" to mean a person that has a covered account with a financial institution or creditor. The Commissions are including this definition for two reasons. First, this definition is the same as the definition of "customer" in the Agencies' final rules. Second, because the definition uses the term "person," it covers 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, not every account held by or offered to a customer will be considered a covered account, as the identification of covered accounts under the identity theft red flags rules is based on a risk-based determination. *See infra* notes 95–100 and accompanying text.

[78] § 162.30(b)(3) (CFTC) and § 248.201(b)(3) (SEC). The Agencies' 2007 Adopting Release (which included an identical definition of the term "account") noted that "the definition of 'account' still applies to fiduciary, agency, custodial, brokerage and investment advisory activities." 2007 Adopting Release *supra* note 8, at 63721.

[79] *See* § 162.30(b)(3)(i).

[80] *See* § 248.201(b)(3)(i).

[81] § 162.30(b)(1) (CFTC) and § 248.201(b)(1) (SEC). Two commenters requested further guidance on the meaning of "continuing relationship" in the proposed definition of the term "account." Comment Letter of Nathaniel Washburn (April 12, 2012); Comment Letter of Chris Barnard ("Chris Barnard Comment Letter") (Mar. 29, 2012). The SEC and the CFTC's definition of "account" is the same as that adopted by the Agencies. The Agencies' 2007 Adopting Release provides further guidance on the meaning of continuing relationship, noting that it is designed to exclude single, non-continuing transactions by non-customers. 2007 Adopting Release *supra* note 8, at 63721.

[82] § 162.30(b)(1).

[83] § 248.201(b)(1).

[84] 77 FR 13450, 13454.

[85] *See* Comment Letter of Kenneth Orgoglioso (May 7, 2012).

[86] *See, e.g.,* 16 CFR 681.1(b)(3).

[87] *See infra* note 93 and accompanying text.

[88] Comment Letter of the American Council of Life Insurers (May 7, 2012); FSR/SIFMA Comment Letter.

[89] FSR/SIFMA Comment Letter.

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

[91] *Id.*

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

definition of "covered account" is deliberately designed to be flexible to allow the financial institution or creditor to determine which accounts pose a reasonably foreseeable risk of identity theft and protect them accordingly. Therefore, we are adopting the definitions of "account" and "covered account" as they were proposed.

The identity theft red flags rules also define several other terms as the Agencies defined them in their final rules, where appropriate, to foster consistent regulations.[93] In addition, terms that the SEC's rules do not define have the same meaning they have in FCRA.[94]

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

As under the proposed rules, under the final rules, each financial institution or creditor must periodically determine whether it offers or maintains covered accounts.[95] As a part of this periodic determination, a financial institution or creditor must conduct a risk assessment that takes into consideration: (1) The methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) its previous experiences with identity theft.[96] A financial institution or creditor should consider whether, for example, a reasonably foreseeable risk of identity theft may exist in connection with accounts it offers or maintains that may be opened or accessed remotely or through methods that do not require face-to-face contact, such as through email or the Internet, or by telephone. In addition, if financial institutions or creditors offer or maintain accounts that have been the target of identity theft, they should factor those experiences into their determination. The Commissions anticipate that entities will be able to demonstrate that they have complied with applicable requirements, including their recurring determinations regarding covered accounts.[97]

The Commissions acknowledge that some financial institutions or creditors regulated by the Commissions do not offer or maintain accounts for personal, family, or household purposes,[98] and engage predominantly in transactions with businesses, where the risk of identity theft is minimal. In these instances, the financial institution or creditor may determine after a preliminary risk assessment that the accounts it offers or maintains do not pose a reasonably foreseeable risk to customers or to its own safety and soundness from identity theft, and therefore it does not need to develop and implement a Program because it does not offer or maintain any "covered accounts." [99] Alternatively, the financial institution or creditor may determine that only a limited range of its accounts present a reasonably foreseeable risk to customers, and therefore may decide to develop and implement a Program that applies only to those accounts or types of accounts.[100] As proposed, under the final rules, a financial institution or creditor that initially determines that it does not need to have a Program is 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 sections 162.30(c) (CFTC) and 248.201(c) (SEC).

2. The Objectives of the Program

The final rules 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.[101] These provisions also 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 final rules are designed to be scalable, by permitting Programs that take into account the operations of smaller institutions. We received no comment on the proposed objectives of the Program and are adopting them as proposed.

3. The Elements of the Program

The final rules set out the four elements that financial institutions and creditors must include in their Programs.[102] These elements are being adopted as proposed and are identical to the elements required under the Agencies' final identity theft red flags rules.[103]

First, the final rules require a financial institution or creditor to develop a Program that includes reasonable policies and procedures to identify relevant red flags [104] for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into the Program.[105] Rather than

[93] *See* § 162.30(b)(4) (CFTC) and § 248.201(b)(4) (SEC) (definition of "credit"); § 162.30(b)(6) (CFTC) and § 248.201(b)(6) (SEC) (definition of "customer"); § 162.30(b)(7) (CFTC) and § 248.201(b)(7) (SEC) (definition of "financial institution"); § 162.30(b)(10) (CFTC) and § 248.201(b)(10) (SEC) (definition of "red flag"); § 162.30(b)(11) (CFTC) and § 248.201(b)(11) (SEC) (definition of "service provider").

The Agencies defined "identity theft" in their identity theft red flags rules 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 defining the terms "identifying information" and "identity theft" by including the same definitions of the terms as they appear in 16 CFR 603.2. *See* § 162.30(b)(8) and (9) (CFTC); § 248.201(b)(8) and (9) (SEC). One commenter suggested that we add the following highlighted language to the definition of "identity theft" so that it would read a "fraud, deception, or other crime committed or attempted using the identifying information of another person without authority." Chris Barnard Comment Letter. Changing the definition of "identity theft" so that it differs from the definition used by the Agencies could lead to higher compliance costs, reduce comparability of the Agencies' rules in contravention of the statutory mandate, and pose difficulties for entities within the enforcement authority of multiple agencies. Accordingly, we are adopting the definition of "identity theft" as it was proposed.

[94] *See* § 248.201(b)(12)(vi) (SEC).

[95] § 162.30(c) (CFTC) and § 248.201(c) (SEC).

[96] § 162.30(c) (CFTC) and § 248.201(c) (SEC).

[97] *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* (noting in joint interpretive guidance provided by the Agencies' staff that, while the Agencies' 2007 identity theft rules do not contain specific record retention requirements, financial institutions and creditors must be able to demonstrate that they have complied with the rules' requirements).

[98] *See* § 162.30(b)(3)(i) (CFTC) and § 248.201(b)(3)(i) (SEC).

[99] *See* § 162.30(b)(3)(ii) (CFTC) and § 248.201(b)(3)(ii) (SEC). For example, an FCM that is otherwise subject to the identity theft red flags rules 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 is otherwise subject to the identity theft 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.

[100] Even a Program limited in scale, however, needs to comply with all of the provisions of the rules. *See, e.g.,* § 162.30(d)–(f) (CFTC) and § 248.201(d)–(f) (SEC) (program requirements).

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

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

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

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

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

Continued

singling out specific red flags as mandatory or requiring specific policies and procedures to identify possible red flags, this first element provides financial institutions and creditors with flexibility in determining which red flags are relevant to their businesses and the covered accounts they manage over time. The list of factors that a financial institution or creditor should consider (as well as examples) are included in Section II of the guidelines, which appear at the end of the final rules.[106] Given the changing nature of identity theft, the Commissions believe that this element allows financial institutions or creditors to respond and adapt to new forms of identity theft and the attendant risks as they arise.

Second, the final rules require financial institutions and creditors to have reasonable policies and procedures to detect the red flags that the Program incorporates.[107] This element does not provide a specific method of detection. Instead, section III of the guidelines provides examples of various means to detect red flags.[108]

Third, the final rules require financial institutions and creditors to have reasonable policies and procedures to respond appropriately to any red flags that they detect.[109] This element incorporates the requirement that a financial institution or creditor assess whether the red flags that are detected evidence a risk of identity theft and, if so, determine how to respond appropriately based on the degree of risk. Section IV of the guidelines sets out a list of aggravating factors and examples that a financial institution or creditor should consider in determining the appropriate response.[110]

Finally, the rules require financial institutions and creditors to have reasonable policies and procedures to periodically update the Program (including the red flags determined to be relevant), to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.[111] As discussed above, financial institutions and creditors are required to determine which red flags are relevant to their businesses and the covered accounts they offer or maintain. The Commissions are requiring a periodic update, rather than immediate or continuous updates, to be parallel with the identity theft red flags rules of the Agencies and to avoid unnecessary regulatory burdens. Section V of the guidelines provides a set of factors that should cause a financial institution or creditor to update its Program.[112] We received no comment on the proposed elements of Programs and are adopting them as proposed.

4. Administration of the Program

The final rules provide direction to financial institutions and creditors regarding the administration of Programs as a means of enhancing the effectiveness of those Programs.[113] First, the final rules require that a financial institution or creditor obtain approval of the initial written Program from either its board of directors, an appropriate committee of the board of directors, or if the entity does not have a board, from a designated senior management employee.[114] This requirement highlights the responsibility of the board of directors in approving a Program. One commenter asked us to clarify that an entity that already has an existing Program in place, in compliance with the other Agencies' rules, need not have the board reapprove the Program to comply with this requirement.[115] We agree that if a financial institution or creditor already has a Program in place, the board is not required to reapprove the existing Program in response to this requirement, provided the Program otherwise meets the requirements of the final rules.

Second, the final rules provide that financial institutions and creditors must involve the board of directors, an appropriate committee thereof, or a designated senior management employee in the oversight, development, implementation, and administration of the Program.[116] The designated senior management employee who is responsible for the oversight of a broker-dealer's, investment company's or investment adviser's Program may be the entity's chief compliance officer.[117] Third, the final rules provide that financial institutions and creditors must train staff, as necessary, to effectively implement their Programs.[118]

Finally, the rules provide that financial institutions and creditors must exercise appropriate and effective oversight of service provider arrangements.[119] The Commissions believe that it is important that the rules address service provider arrangements so that financial institutions and creditors remain legally responsible for compliance with the rules, irrespective of whether such financial institutions and creditors outsource their identity theft red flags detection, prevention, and mitigation operations to a service provider.[120] The final rules do not prescribe a specific manner in which appropriate and effective oversight of service provider arrangements must occur. Instead, the requirement provides flexibility to financial institutions and creditors in maintaining their service provider arrangements, while making clear that such institutions and creditors are still required to fulfill their legal compliance obligations.[121] We received no comments on the substance of this aspect of the proposal [122] and are adopting the requirements related to the administration of Programs as proposed.

determination, the board (or committee 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. *See* 2007 Adopting Release, *supra* note 8, at 63730.

[106] *See* Section II.B.2 below.

[107] *See* § 162.30(d)(2)(ii) (CFTC) and § 248.201(d)(2)(ii) (SEC).

[108] *See* Section II.B.3 below.

[109] *See* § 162.30(d)(2)(iii) (CFTC) and § 248.201(d)(2)(iii) (SEC).

[110] *See* Section II.B.4 below.

[111] *See* § 162.30(d)(2)(iv) (CFTC) and § 248.201(d)(2)(iv) (SEC).

[112] *See* Section II.B.5 below.

[113] *See* § 162.30(e) (CFTC) and § 248.201(e) (SEC).

[114] *See* § 162.30(e)(1) (CFTC) and § 248.201(e)(1) (SEC), *see also* § 162.30(b)(2) (CFTC) and § 248.201(b)(2) (SEC).

[115] ICI Comment Letter.

[116] *See* § 162.30(e)(2) (CFTC) and § 248.201(e)(2) (SEC). Section VI of the guidelines elaborates on this provision.

[117] *See, e.g.*, rule 38a–1(a)(4) under the Investment Company Act (addressing the chief compliance officer position), 17 CFR 270.38a–1(a)(4); rule 206(4)–7(c) under the Investment Advisers Act, 17 CFR 275.206(4)–7 (same).

[118] *See* § 162.30(e)(3) (CFTC) and § 248.201(e)(3) (SEC).

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

[120] For example, a financial institution or creditor that uses a service provider to open accounts on its 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 remains responsible for ensuring that the activity is conducted in compliance with a Program that meets the requirements of the identity theft red flags rules.

[121] These legal compliance obligations include, but are not limited to, the maintenance of records in connection with any service provider arrangements. *See* 17 CFR 240.17a–4(b)(7) (requiring that each broker-dealer maintain a record of all written agreements entered into by the broker-dealer relating to its business as such); 17 CFR 275.204–2(a)(10) (requiring that each investment adviser maintain a record of all written agreements entered into by the investment adviser with any client or otherwise relating to the business of the investment adviser as such).

[122] *But see infra* note 143 and accompanying text (discussing a comment received on the costs associated with this aspect of the proposal).

B. Final Guidelines

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

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

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

Section I of the guidelines makes clear that a financial institution or creditor may incorporate into its Program, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft. An example of such existing policies, procedures, and other arrangements may include other policies, procedures, and arrangements that the financial institution or creditor has developed to prevent fraud or otherwise ensure compliance with applicable laws and regulations.

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

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

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

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

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- Presentation of suspicious documents, such as documents that appear to have been altered or forged;
- Presentation of suspicious personal identifying information, such as a suspicious address change;
- Unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

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

3. Section III of the Guidelines—Detecting Red Flags

Section III of the guidelines provides examples of policies and procedures that a financial institution or creditor must consider including in its Program's policies and procedures for the purpose of detecting red flags. As discussed in the Proposing Release, entities that are currently subject to the Agencies' identity theft red flags rules,[125] the federal customer identification program ("CIP") rules [126] or other Bank Secrecy Act rules,[127] the Federal Financial Institutions Examination Council's guidance on authentication,[128] or the Interagency Guidelines Establishing Information Security Standards [129] may already be engaged in detecting red flags. These entities may wish to integrate the policies and procedures already developed for purposes of complying with these rules and standards into their Programs. However, such policies and procedures may need to be supplemented.[130]

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

Section IV of the guidelines states that a Program's policies and procedures should provide for appropriate responses to the red flags that a financial institution or creditor has detected, that are commensurate with the degree of risk posed by each red flag. In determining an appropriate response, under the guidelines, a financial institution or creditor is required to consider aggravating factors that may heighten the risk of identity theft. Section IV of the guidelines also provides several examples of appropriate responses. These examples are identical to those included in the Agencies' final guidelines. Financial institutions and creditors also may consider adopting measures to prevent and mitigate identity theft that are not listed in the guidelines.

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

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

[123] 15 U.S.C. 1681m(e)(1)(A).

[124] *See* § 162.30(f) (CFTC) and § 248.201(f) (SEC).

[125] *See* 2007 Adopting Release, *supra* note 8.

[126] *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).

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

[128] *See* "Authentication in an Internet Banking Environment," *available at http://www.ffiec.gov/pdf/authentication_guidance.pdf.*

[129] *See* 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D–2 and part 225, app. F (state member banks and bank holding companies); 12 CFR part 364, app. B (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, app. A (credit unions).

[130] For example, the CIP rules were written to implement section 326 (31 U.S.C. 5318(*l*)) of the USA PATRIOT Act (Pub. L. 107–56 (2001)), and certain types of "accounts," "customers," and products are exempted or treated specially in the CIP rules because they pose a lower risk of money laundering or terrorist financing. Such special treatment may not be appropriate to accomplish the broader objective of detecting, preventing, and mitigating identity theft.

identity theft; (iii) changes in methods to detect, prevent, and mitigate identity theft; (iv) changes in the types of accounts that the financial institution or creditor offers or maintains; and (v) changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

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

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

i. Oversight of Identity Theft Prevention Program

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

ii. Reporting to the Board of Directors

Section VI(b) of the guidelines states that staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated senior management employee, at least annually, on compliance by the financial institution or creditor with the final rules. In addition, section VI(b) of the guidelines provides that the report should address material matters related to the Program and evaluate issues such as recommendations for material changes to the Program.[131]

iii. Oversight of Service Provider Arrangements

Section VI(c) of the guidelines provides that whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. As discussed in the Proposing Release, the Commissions believe that these guidelines make clear that a service provider that provides services to multiple financial institutions and creditors may do so in accordance with its own program to prevent identity theft, as long as the service provider's program meets the requirements of the identity theft red flags rules.

Section VI(c) of the guidelines also includes, as an example of how a financial institution or creditor may comply with this provision, that a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities, and either report the red flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft. In those circumstances, the Commissions expect that the contractual arrangements would include the provision of sufficient documentation by the service provider to the financial institution or creditor to enable it to assess compliance with the identity theft red flags rules.

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

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

8. Supplement A to the Guidelines

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

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

C. Final Card Issuer Rules

Section 615(e)(1)(C) of the FCRA provides that the CFTC and SEC must "prescribe regulations applicable to card issuers to ensure that, if a card issuer receives notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after such notification is received) receives a request for an additional or replacement card for the same account, the card issuer may not issue the additional or replacement card, unless the card issuer applies certain address validation procedures."[132] Accordingly, the Commissions are adopting rules that set out the duties of card issuers regarding changes of address.[133] These rules are similar to the final card issuer rules adopted by the Agencies.[134] The rules apply only to a person that issues a debit or credit card ("card issuer") and that is subject to the enforcement authority of either Commission.[135] The Commissions did not receive any comments on the card issuer rules, and are adopting them as proposed.

As discussed in the Proposing Release, the CFTC is not aware of any entities subject to its enforcement authority that issue debit or credit cards and, as a matter of practice, believes that it is highly unlikely that CFTC-regulated entities would issue debit or credit cards. As also discussed in the Proposing Release, the SEC understands that a number of entities within its enforcement authority issue cards in partnership with affiliated or unaffiliated banks and financial institutions, but that these cards are generally issued by the partner bank, and not by the SEC-regulated entity. The SEC therefore expects that no entities within its enforcement authority will be subject to the card issuer rules.

[131] The other issues referenced in the guideline are: (i) The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; (ii) service provider arrangements; and (iii) significant incidents involving identity theft and management's response.

[132] 15 U.S.C. 1681m(e)(1)(C).

[133] *See* § 162.32 (CFTC) and § 248.202 (SEC).

[134] *See, e.g.*, 16 CFR 681.3 (FTC).

[135] *See supra* Section II.A.1.

III. Related Matters

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

CFTC

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

Cost-Benefit Considerations of Identity Theft Red Flags Rules

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

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

Comments. The CFTC received two comments on its consideration of the costs and benefits of the joint proposal. These two commenters were divided on the reasonableness of the Commissions' estimated costs of compliance. In a letter focused on the SEC's proposed regulations (which are, of course, substantially similar to the CFTC's proposed regulations), one commenter stated that because Regulation S–ID "is substantially similar to" the existing FTC rules and guidelines, broker-dealers should not bear "any new costs in coming into compliance with proposed Regulation S–ID."[139] This commenter further stated that "broker-dealers should already have in place a program that complies with the FTC rule. While firms will need to update some of their procedures to reflect the SEC's new responsibility for the oversight of the application of this rule, many of the changes would be cosmetic and grammatical in nature." [140] In marked contrast, another comment letter, submitted on behalf of the Financial Services Roundtable ("FSR") and the Securities Industry and Financial Markets Association ("SIFMA"), stated that the "consensus of our members is that the estimated compliance costs for the proposed Rules are extremely low and unrealistic." [141]

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

The FSR/SIFMA Comment Letter also stated that "financial institutions with an existing Red Flags program would experience an incremental burden due to reassessing the scope of the 'covered accounts' and reevaluating whether a business activity would be defined as a 'financial institution' or as a 'creditor' for purposes of the Agencies' Rules."[142] The letter did not attribute a time estimate to this "incremental burden."

Finally, the FSR/SIFMA Comment Letter contended that the Commissions' "estimated compliance costs further fail to consider the cost to third-party service providers, many of which may be required to implement an identity theft program even though they are not financial institutions or creditors." [143]

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

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

[136] 7 U.S.C. 19(a).

[137] *Id.*

[138] 77 FR 13450 (Mar. 6, 2012).

[139] *See* NSCP Comment Letter.

[140] *Id.*

[141] *See* FSR/SIFMA Comment Letter.

[142] *Id.*

[143] *Id.*

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

[145] *See* NSCP Comment Letter.

[146] *See supra* note 142 and accompanying text.

[147] *See* FSR/SIFMA Comment Letter.

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

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

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

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

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

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

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

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

[148] *See* OCC Comment Letter.

[149] *See infra* notes 151 and 152.

[150] *See supra* notes 95–100 and accompanying text.

[151] 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 × 12 hours = $4,248; $66 × 17 = $1,122; $4,000 × 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 168 and text following note 168. CFTC staff estimates that 2 hours of internal counsel's time would be spent conducting an initial assessment to determine whether they have covered accounts and whether they are subject to the proposed rule (or 702 entities). The cost associated with this determination is $497,016 based on the following calculation: $354 × 2 = $708; $708 × 702 = $497,016. CFTC staff estimates that 54 entities would bear the remaining specified costs for a total cost of $683,748 (54 × $12,662 = $683,748). *See* SIFMA's Office Salaries in the Securities Industry 2011.

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

[152] 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 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 × 7 hours = $2,478; $4,000 × 1 hour = $4,000; $2,478 + $4,000 = $6,478 ≈ $6,500.

As discussed in the PRA analysis, CFTC staff estimates that 2,946 existing CFTC-regulated entities would be financial institutions or creditors, of which 260 maintain covered accounts. CFTC staff estimates that 2 hours of internal counsel's time would be spent conducting periodic assessments of covered accounts and that all financial institutions or creditors subject to the proposed rule (or 2,946 entities) would bear this cost for a total cost of $2,100,000 based on the following calculations rounded to two significant digits: $354 × 2 = $708; $708 × 2,946 = $2,085,768 ≈ $2,100,000. CFTC staff estimates that 260 entities would bear the remaining specified ongoing costs for a total cost of $1,500,000 (260 × $5,770 = $1,500,200 ≈ $1,500,000).

deterred or prevented is not knowable. The CFTC, however, recognizes that the cost of any given instance of identity theft may be substantial to the individual involved. Joint adoption of identity theft red flags rules in a form that is substantially similar to the Agencies' identity theft red flags rules might also benefit financial institutions and creditors because entities regulated by multiple federal agencies could comply with a single set of standards, which would reduce potential compliance costs. As is true of the Agencies' identity theft red flags rules, the CFTC has designed section 162.30 to provide financial institutions and creditors significant flexibility in developing and maintaining a Program that is tailored to the size and complexity of their business and the nature of their operations, as well as in satisfying the address verification procedures.

Accordingly, as previously discussed, section 162.30 should not result in any significant new costs or benefits, because it 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 detecting, preventing, and mitigating identity theft, an illegal act that may be costly to them in both time and money.[153] Because, however, these rules create no new requirements — rather, as explained above, the CFTC is adopting rules that reflect requirements already in place — the impact of the rules on the protection of market participants and the public will remain the same. The Commission is not aware of any effect of these rules on the efficiency, competitiveness, and financial integrity of futures markets, price discovery, sound risk management practices, or other public interest considerations. Customers of CFTC registrants will continue to benefit from these rules in the same way they have benefited from the rules as they were administered by the Agencies.

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 credit and debit card issuers as being a possible indicator of identity theft. Accordingly, the card issuer rules in section 162.32 set out the duties of card issuers regarding changes of address. The card issuer rules will apply only to a person that issues a debit or credit card and that is subject to the CFTC's enforcement authority. The card issuer rules require a card issuer to comply with certain address validation procedures in the event that such issuer receives a notification of a change of address for an existing account 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.

Section 162.32 will 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 January 1, 2011. Because section 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 section 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 section 162.32.

The benefits related to adoption of section 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 estimate with precision the dollar value associated with the benefits that will inure to the public from these card issuer rules. As is true of the Agencies' card issuer rules, the CFTC has designed section 162.32 to provide card issuers significant flexibility in developing and maintaining a Program that is tailored to the size and complexity of their business and the nature of their operations.

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

Section 15(a) Analysis. As stated above, the CFTC is required to consider costs and benefits of proposed CFTC action in light of (1) Protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. These rules protect market participants and the public by preventing identity theft, an illegal act that may be costly to them in both time and money.[154] 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 rules in the same way they have benefited from the rules as they were administered by the Agencies.

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

[154] *See id.*

SEC

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

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

Section 615(e)(1)(C) of the FCRA singles out change of address notifications sent to credit and debit card issuers as a possible indicator of identity theft, and requires the SEC to prescribe regulations concerning such notifications. Accordingly, the card issuer rules in this release set out the duties of card issuers regarding changes of address. The card issuer rules apply only to SEC-regulated entities that issue credit or debit cards.[155] The card issuer rules require a card issuer to comply with certain address validation procedures in the event that such issuer receives a notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after it receives such notification) receives a request for an additional or replacement card for the same account. The card issuer may not issue the additional or replacement card unless it complies with those procedures. The procedures include: (1) Notifying the cardholder of the request either at the cardholder's former address, or by any other means of communication that the card issuer and the cardholder have previously agreed to use; or (2) assessing the validity of the change of address in accordance with established policies and procedures.

The baseline we use to analyze the economic effects of Regulation S–ID is the identity theft red flags regulatory scheme administered by the Agencies. Regulation S–ID, as discussed above, implements the transfer of oversight of identity theft red flags rules for SEC-regulated entities from the Agencies to the SEC. Entities that qualify as a financial institution or creditor and offer or maintain covered accounts should already have existing identity theft red flags Programs. Regulation S–ID does not contain new requirements, nor does it expand the scope of the Agencies' rules to include new entities that the Agencies' rules did not previously cover. Regulation S–ID does contain examples and minor language changes designed to help guide entities within the SEC's enforcement authority in complying with the rules. Because Regulation S–ID is substantially similar to the Agencies' rules, the entities within its scope should not bear new costs in coming into compliance with Regulation S–ID.[156]

Costs

The costs of complying with section 248.201 of Regulation S–ID include both ongoing costs and initial, one-time costs.[157] These are the same costs that were associated with the requirements of the Agencies' red flags rules, and these costs will continue to apply after the adoption of the SEC's identity theft red flags rules (section 248.201 of Regulation S–ID). The ongoing costs include the costs to periodically review and update the Program, report on the Program, and conduct assessments of covered accounts.[158] All entities that qualify as financial institutions or creditors and that maintain covered accounts will bear these costs. Existing entities subject to Regulation S–ID should already bear, and will continue to be subject to, the ongoing costs.

Initial, one-time costs relate to the initial assessments of covered accounts, creation of a Program, board approval of the Program, and the training of staff.[159] New entities will bear these costs.

[155] *See* § 248.202(a) (defining scope of the SEC's rules).

[156] *See, e.g.*, NSCP Comment Letter ("Because proposed Regulation S–ID is substantially similar to [the Agencies'] existing rules and guidelines, broker-dealer firms should not bear any new costs in coming into compliance with proposed Regulation S–ID."). As previously indicated, the SEC staff understands that a number of investment advisers may not currently have identity theft red flags Programs. *See supra* note 55 and *infra* notes 186 and 190. The new guidance in this release may lead some of these entities to determine that they should comply with Regulation S–ID. Although the costs and benefits of Regulation S–ID discussed below would be new to these entities, the costs would result not from Regulation S–ID but instead from the entities' recognition that these rules and the previously-existing rules apply to them. In that regard, the initial, one-time costs of Regulation S–ID could be up to $756 for each investment adviser that qualifies as a financial institution or creditor, and additional one-time costs of $13,885 for each such investment adviser that maintains covered accounts. *See infra* notes 158 and 159. Not all investment advisers will bear the full extent of these costs, however, as some may already have in place certain identity theft protections. And, the guidance in this release could have the benefit of further reducing identity theft. *See infra* discussion of benefits in Part III.A of this release.

[157] *See infra* note 182 and accompanying text.

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

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

As discussed in the PRA analysis, SEC staff estimates that 10,339 existing SEC-regulated entities will be financial institutions or creditors under Regulation S–ID, and approximately 90%, or 9305, of these entities will maintain covered accounts. *See infra* notes 190 and 191 and accompanying text. SEC staff estimates that 2 hours of internal counsel's time will be spent conducting periodic assessments of covered accounts and that all financial institutions or creditors subject to the rule (or 10,339 entities) will bear this cost for a total cost of $7,816,284 based on the following calculations: $378 × 2 = $756; $756 × 10,339 = $7,816,284. SEC staff estimates that 9305 entities will bear the remaining specified ongoing costs for a total cost of $59,458,950 (9305 × (($378 × 5) + ($4500 × 1)) = $59,458,950).

[159] SEC staff estimates that the incremental one-time burden of compliance includes 2 hours to conduct initial assessments of covered accounts, 25 hours to develop and obtain board approval of a Program, and 4 hours to train staff. SEC staff estimates that, of the 31 hours incurred, 12 hours will be spent by internal counsel at an hourly rate of $378, 17 hours will be spent by administrative

As discussed above, the final rules require financial institutions and creditors to tailor their Programs to the size and complexity of the entity and to the nature and scope of the entity's activities. Ongoing and one-time costs will therefore depend on the size and complexity of the SEC-regulated entity. Entities may already have other policies and procedures in place that are designed to reduce the risks of identity theft for their customers. The presence of other related policies and procedures could reduce the ongoing and one-time costs of compliance.

Two commenters agreed with the SEC that the substantial similarity of Regulation S–ID to the Agencies' rules should minimize any compliance costs for entities that have previously complied with the Agencies' rules,[160] and another commenter stated that the benefits of reduced risk of identity theft would outweigh the costs associated with the rules.[161] Another commenter raised concerns with the cost estimates in the Proposing Release, and argued that actual costs of compliance could be much greater than estimated.[162] This commenter provided hour burden estimates for large, complex financial institutions that were significantly higher than the estimates made for those entities in the Proposing Release. Additionally, the commenter stated that the Commissions' estimated compliance costs did not consider the costs to third-party service providers that may be required to implement an identity theft red flags Program, even though they are not financial institutions or creditors. The commenter also noted, however, that burdens placed upon entities currently complying with the Agencies' rules would be the same burdens that each of these entities already incurs in regularly assessing whether it maintains covered accounts and evaluating whether it falls within the rules' scope.

We note that the commenter who suggested that significantly higher hour burdens would be associated with the rules focused on large, complex financial institutions. Regulation S–ID requires each financial institution and creditor to tailor its Program to its size and complexity, and to the nature and scope of its activities. Our estimates take into account the hour burdens for small financial institutions and creditors, which we understand, based on discussions with industry representatives, to be significantly less than the estimates provided by this commenter. We also note that costs to service providers have already been taken into account, as SEC-regulated entities that have outsourced identity theft detection, prevention, and mitigation operations to service providers have effectively shifted a burden that the SEC-regulated entities otherwise would have carried themselves.[163] As mentioned above, the costs of Regulation S–ID are not new, and existing entities should already have identity theft red flags Programs and bear the ongoing costs associated with Regulation S–ID.

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

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

Benefits

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

Alternatives

In analyzing the costs and benefits that could result from the implementation of Regulation S–ID, the

assistants at an hourly rate of $65, and 2 hours will be spent by the board of directors as a whole, at an hourly rate of $4500, for a total cost of $14,641 per new entity. This estimate is based on the following calculations: $378 × 12 hours = $4536; $65 × 17 = $1105; $4500 × 2 = $9000; $4536 + $1105 + $9000 = $14,641. The cost estimate for administrative assistants is derived from SIFMA's Office Salaries in the Securities Industry 2011, modified to account for an 1800-hour work-year and multiplied by 2.93 to account for bonuses, entity size, employee benefits, and overhead.

As discussed in the PRA analysis, SEC staff estimates that there are 1271 SEC-regulated entities that newly form each year and that could be financial institutions or creditors, of which 668 are likely to qualify as financial institutions or creditors. *See infra* note 186. Of these 668 entities that are likely to qualify as financial institutions or creditors, SEC staff estimates that approximately 90%, or 601, of these entities will maintain covered accounts. *See infra* note 188 and accompanying text. SEC staff estimates that 2 hours of internal counsel's time will be spent conducting an initial assessment of covered accounts and that all newly-formed financial institutions or creditors subject to Regulation S–ID (or 668 entities) will bear this cost for a total cost of $505,008 based on the following calculation: $378 × 2 = $756; $756 × 668 = $505,008. SEC staff estimates that the 601 entities that will maintain covered accounts will bear the remaining specified costs for a total cost of $8,344,885 (601 × (($378 × 10) + ($65 × 17) + ($4500 × 2)) = $8,344,885).

[160] *See* NSCP Comment Letter ("Because proposed Regulation S–ID is substantially similar to [the Agencies'] existing rules and guidelines, broker-dealer firms should not bear any new costs in coming into compliance with proposed Regulation S–ID."); ICI Comment Letter ("We commend the Commission for proposing requirements that are consistent with those that have applied to certain SEC registrants since 2008 pursuant to rules of the [FTC] under [the FACT Act]. This consistency will facilitate registrants' transition from compliance with the FTC's rule to the Commission's rule with little or no disruption or added expense.")

[161] *See* Eric Speicher Comment Letter.

[162] *See* FSR/SIFMA Comment Letter. FSR/SIFMA estimated that "the initial compliance burden to implement the [proposed rules] would average 2,000 hours for each line of business conducted by a large, complex financial institution . . ." and that "the continuing compliance monitoring for a large, complex financial institution . . . would average 400 hours annually." FSR/SIFMA also noted that "financial institutions with an existing Red Flags program would experience an incremental burden" in connection with the SEC's rules.

[163] *See infra* Section III.C. (describing the SEC's PRA collection of information requirements).

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

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

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

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

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

[164] *See infra* Section IV (setting forth statutory authority under, among other things, the Exchange Act and Investment Company Act for rulemakings).

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

C. Paperwork Reduction Act

CFTC

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

1. Information Provided by Reporting Entities/Persons

Under part 162, subpart C, CFTC regulated entities—which presently would include approximately 260 CFTC registrants [166] plus 125 new CFTC registrants pursuant to Title VII of the Dodd-Frank Act [167]—are required to design, develop and implement reasonable policies and procedures to identify relevant red flags, and potentially to notify cardholders of identity theft risks. In addition, CFTC-regulated entities are required to: (i) Collect information and keep records for the purpose of ensuring that their Programs met requirements to detect, prevent, and mitigate identity theft in

[166] *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 November 20, 2012. The NFA's site states that there are 3,485 CFTC registrants as of October 31, 2012. (The total number of registrants also includes 7 exchanges which are not subject to this rule and not included in the calculation.) Of the 3,485 registrants, there are 104 FCMs, 1,284 IBs, 1,041 CTAs, 1,035 CPOs, and 14 RFEDs. CFTC staff has observed that approximately 50 percent of all CPOs (518) are dually registered as CTAs. Moreover, CFTC staff also has observed that all entities registering as RFEDs (14) also register as FCMs. Based on these observations, the CFTC has determined that the total number of entities is 2,946 (this total excludes the 7 exchanges that are not subject to this rule, the 518 CPOs that are also registered as CTAs, and the 14 RFEDs that are also registered as FCMs).

Of the total 2,946 entities, all of the FCMs (104) are likely to qualify as financial institutions or creditors carrying covered accounts, approximately 10 percent of CTAs (104) and CPOs (52) 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 260 financial institutions or creditors that would bear the initial one-time burden of compliance with the CFTC's rules.

[167] CFTC staff estimates that 125 SDs and MSPs will register with the CFTC upon 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.

connection with the opening of a covered account or any existing covered account; (ii) develop and implement reasonable policies and procedures to identify, detect and respond to relevant red flags, as well as periodic reports related to the Program; and (iii) from time to time, notify cardholders of possible identity theft with respect to their covered accounts, as well as assess the validity of those accounts.

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

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

i. Initial Burden

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

The CFTC estimates that approximately 702 FCMs, CTAs and CPOs [168] 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.[169] Of these 827 entities, CFTC staff estimates that approximately 179 of these entities may maintain covered accounts. Accordingly, the CFTC estimates the one-time burden for these 179 entities to be 5,191 hours,[170] for a total burden among newly registered entities of 6,845 hours.[171]

ii. Ongoing Burden

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

The CFTC estimates that approximately 3,071 entities may maintain covered accounts, and that they would be required to periodically review their accounts to determine if they comply with these rules, for a total of 6,142 hours for these entities.[172] Of these 3,071 entities, the CFTC estimates that approximately 385 maintain covered accounts, and thus would need to incur the additional burdens related to complying with the rule, for a total of 2,310 hours.[173] The total ongoing burden for all CFTC registrants is 8,452 hours.[174]

SEC:

Provisions of sections 248.201 and 248.202 contain ''collection of information'' requirements within the meaning of the PRA. In the Proposing Release, the SEC solicited comment on the collection of information requirements. The SEC also submitted the proposed collections of information to the OMB for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. The title for this collection of information is ''Part 248, Subpart C—Regulation S–ID.'' In response to this submission, the OMB issued control number 3235–0692.[175] Responses to the new collection of information provisions are mandatory, and the information, when provided to the SEC in connection with staff examinations or investigations, is kept confidential to the extent permitted by law.

1. Description of the Collections

Under Regulation S–ID, SEC-regulated entities are required to develop and implement reasonable policies and procedures to identify, detect and respond to relevant red flags and, in the case of entities that issue credit or debit cards, to assess the validity of, and communicate with cardholders regarding, address changes. Section 248.201 of Regulation S–ID includes the following ''collections of information'' by SEC-regulated entities that are financial institutions or creditors if the entity maintains covered accounts: (1) Creation and periodic updating of a Program that is approved by the board of directors, an appropriate committee thereof, or a designated senior management employee; (2) periodic staff reporting on compliance with the identify theft red flags rules and guidelines, as required to be considered by section VI of the guidelines; and (3) training of staff to implement the Program. Section 248.202 of Regulation S–ID includes the following ''collections of information'' by SEC-regulated entities that are credit or debit card issuers: (1) Establishment of policies and procedures that assess the validity

[168] 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. With respect to RFEDs, CFTC staff has observed that all entities registering as RFEDs also register as FCMs. Based on these observations, 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). Each of these 702 financial institutions or creditors would bear the initial one-time burden of compliance with the proposed 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.

[169] This estimate is based on the following calculation: 827 entities × 2 hours = 1,654 hours.

[170] This estimate is based on the following calculation: 179 entities × 29 hours = 5,191 hours.

[171] This estimate is based on the following calculation: 1,654 hours for all newly registered CFTC registrants + 5,191 hours for the one-time burden of newly registered entities with covered accounts, for a total of 6,845 hours.

[172] This estimate is based on the following calculation: 3,071 entities x 2 hours = 6,142 hours. (The Proposing Release contained an arithmetic error in the calculation for the total ongoing burden for all CFTC registrants. The total number of hours was erroneously calculated to total 76,498 hours rather than 6,498. *See* 77 FR 13450, 13467.)

[173] This estimate is based on the following calculation: 385 entities x 6 hours = 2,310 hours.

[174] This estimate is based on the following calculation: 6,142 hours + 2,310 hours = 8,452 hours.

[175] 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.

of a change of address notification if a request for an additional or replacement card on the account follows soon after the address change; and (2) notification of a cardholder, before issuance of an additional or replacement card, at the previous address or through some other previously agreed-upon form of communication, or alternatively, assessment of the validity of the address change request through the entity's established policies and procedures.

SEC-regulated entities that must comply with the collections of information required by Regulation S–ID should already be in compliance with the identity theft red flags rules that the Agencies jointly adopted in 2007.[176] The requirements of those rules are substantially similar and comparable to the requirements of Regulation S–ID.[177]

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

SEC staff estimates of time and cost burdens represent the one-time burden of complying with Regulation S–ID for newly-formed SEC-regulated entities, and the ongoing costs of compliance for all SEC-regulated entities.[182] SEC staff estimates also attribute all burdens to entities that are directly subject to the requirements of the rulemaking. An entity directly subject to Regulation S–ID that outsources activities to a service provider is, in effect, shifting to that service provider the burden that it would otherwise have carried itself. Under these circumstances, the burden is, by contract, shifted from the entity that is directly subject to Regulation S–ID to the service provider, but the total amount of burden is not increased. Thus, service provider burdens are already included in the burden estimates provided for entities that are directly subject to Regulation S–ID. The time and cost estimates made here are based on conversations with industry representatives and on a review of comments received on the proposed rules as well as the estimates made in the regulatory analyses of the identity theft red flags rules previously issued by the Agencies.

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

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

i. Initial Burden

SEC staff estimates that the one-time burden of compliance with section 248.201 for SEC-regulated financial institutions and creditors with covered accounts is: (i) 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 will be spent by internal counsel, 17 hours will be spent by administrative assistants, and 2 hours will be spent by the board of directors as a whole for newly-formed entities.

SEC staff estimates that approximately 668 SEC-regulated financial institutions and creditors are newly formed each year.[186] Each of these 668 entities will need to conduct an initial assessment of covered accounts, for a total of 1336 hours.[187] Of these 668 entities, SEC staff estimates that approximately 90% (or

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

[177] *See* 2007 Adopting Release, *supra* note 8, at Section VI.A (discussing the PRA analysis with respect to the Agencies' identity theft red flags rules); "FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule" at *http://www.ftc.gov/opa/2010/05/redflags.shtm.*

[178] 31 U.S.C. 5318(l) (requiring verification of the identity of persons opening accounts).

[179] 15 U.S.C. 6801.

[180] 15 U.S.C. 1681w.

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

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

[183] § 248.201(a).

[184] *See* 2007 Adopting Release, *supra* note 8, at Section VI.A (discussing the PRA analysis with respect to the Agencies' identity theft red flags rules). Because the requirements of Regulation S–ID are substantially identical to the requirements of the Agencies' identity theft red flags rules, the SEC staff took the Agencies' PRA analysis into account in estimating the regulatory burdens of Regulation S–ID.

[185] *See supra* note 162 and accompanying text.

[186] Based on a review of new registrations typically filed with the SEC each year, SEC staff estimates that approximately 900 investment advisers, 231 broker-dealers, 139 investment companies, and 1 ESC typically apply for registration with the SEC or otherwise are newly formed each year, for a total of 1271 entities that could be financial institutions or creditors. Of these, SEC staff estimates that all of the investment companies, ESCs, and broker-dealers are likely to qualify as financial institutions or creditors, and 33% (or 297) of investment advisers are likely to qualify, for a total of 668 total financial institutions or creditors that will bear the initial one-time burden of assessing covered accounts under Regulation S–ID. Information regarding the method used to estimate that 33% of investment advisers are likely to qualify as financial institutions or creditors can be found in note 190 below.

[187] This estimate is based on the following calculation: 668 entities × 2 hours = 1336 hours.

601) maintain covered accounts.[188] Accordingly, SEC staff estimates that the total initial burden for the 601 newly formed SEC-regulated entities that are likely to qualify as financial institutions or creditors and maintain covered accounts is 18,631 hours, and the total initial burden for all newly formed SEC-regulated entities is 18,765 hours.[189]

ii. Ongoing Burden

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

SEC staff estimates that there are 10,339 SEC-regulated entities that are either financial institutions or creditors, and that all of these are required to periodically review their accounts to determine if they offer or maintain covered accounts, for a total of 20,678 hours for these entities.[190] Of these 10,339 entities, SEC staff estimates that approximately 90%, or 9305, maintain covered accounts, and thus will bear the additional burdens related to complying with the rules.[191] Accordingly, SEC staff estimates that the total ongoing burden for these 9305 financial institutions and creditors that maintain covered accounts will be 74,440 hours.[192] The estimated total ongoing burden for the 10,339 SEC-regulated entities that are financial institutions or creditors covered by Regulation S–ID will be 76,508 hours.[193]

2. *Section 248.202 (Duties of Card Issuers Regarding Changes of Address).*

The collections of information required by section 248.202 apply only to SEC-regulated entities that issue credit or debit cards.[194] SEC staff understands that SEC-regulated entities generally do not issue credit or debit cards, but instead have arrangements with other entities, such as banks, that issue cards on their behalf. These other entities, which are not regulated by the SEC, are already subject to substantially similar change of address obligations pursuant to the Agencies' identity theft red flags rules. In addition, SEC staff understands that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Therefore, implementation of this requirement poses no further burden.

SEC staff does not expect that any SEC-regulated entities will be subject to the information collection requirements of section 248.202. Accordingly, SEC staff estimates that there is no hourly or cost burden for SEC-regulated entities related to section 248.202. In the Proposing Release, the SEC solicited comment on this same estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.

D. Regulatory Flexibility Act

CFTC

The Regulatory Flexibility Act ("RFA") requires that federal agencies consider whether the rules they propose will have a significant economic impact on a substantial number of small entities and, if so, provide a regulatory flexibility analysis respecting the impact.[195] The CFTC has already established certain definitions of "small entities" to be used in evaluating the impact of its rules on such small entities in accordance with the RFA.[196] The CFTC's final identity theft red flags regulations affect FCMs, RFEDs, IBs, CTAs, CPOs, SDs, and MSPs. SDs and MSPs are new categories of registrants. Accordingly, the CFTC has noted in other rule proposals that it has not previously addressed the question of whether such persons were, in fact, small entities for purposes of the RFA.[197]

In this regard, the CFTC has previously determined that FCMs should not be considered to be small entities for purposes of the RFA, based, in part, upon FCMs' obligation to meet the minimum financial requirements established by the CFTC to enhance the protection of customers' segregated funds and protect the financial condition of FCMs generally.[198] Like FCMs, SDs will be subject to minimum capital and margin requirements, and

[188] In the Proposing Release, the SEC requested comment on the estimate that approximately 90% of all financial institutions and creditors maintain covered accounts; the SEC received no comments on this estimate.

[189] These estimates are based on the following calculations: 601 financial institutions and creditors that maintain covered accounts × 31 hours = 18,631 hours; 17,429 hours (601 financial institutions and creditors that maintain covered accounts x 29 hours) + 1336 hours (burden for all SEC-regulated entities that are financial institutions or creditors to conduct an initial assessment of covered accounts) = 18,765 hours.

[190] Based on a review of entities that the SEC regulates, SEC staff estimates that, as of July 1, 2012, there are approximately 11,622 investment advisers, 4706 broker-dealers, 1692 active open-end investment companies, and 150 ESCs. Of these, SEC staff estimates that all of the broker-dealers, open-end investment companies and ESCs are likely to qualify as financial institutions or creditors, and approximately 3791 investment advisers (or about 33%, as explained further below) are likely to qualify, for a total of 10,339 total financial institutions or creditors that will bear the ongoing burden of assessing covered accounts under Regulation S–ID. (The SEC staff estimates that the other types of entities that are covered by the scope of the SEC's rules will not be financial institutions or creditors and therefore will not be subject to the rules' requirements. *See supra* note 182.) The total hours estimate is based on the following calculation: 10,339 entities × 2 hours = 20,678 hours.

The SEC staff estimate that 33% of SEC-registered investment advisers will be subject to the requirements of Regulation S–ID is based on the following calculation. According to Investment Adviser Registration Depository (IARD) data, there are approximately 11,622 investment advisers registered with the SEC as of July 1, 2012. Of these advisers, approximately 7327 could potentially be subject to the rule as financial institutions because they indicate they have customers who are natural persons. We estimate that approximately 16%, or 1202 of these 7327 advisers, hold transaction accounts belonging to natural persons and therefore would qualify as financial institutions under the rule. Additionally, 4055 of the 11,622 advisers registered with the SEC have private fund clients. We expect that most of the funds advised by these advisers would have at least one natural person investor, and thus they could potentially meet the definition of "financial institution." In addition, some of these private fund advisers may engage in lending activities that would also qualify them as creditors under the rule. In order to avoid duplication, however, we are deducting 1466 private fund advisers from the total number of advisers we estimate will be subject to the rule, because they also indicated on Form ADV that they have individual or high net worth clients and are already accounted for in our estimates above. Accordingly, the staff estimates that approximately 3791 (*i.e.*, 1202 + 4055 − 1466) advisers registered with the SEC will be subject to the rule. These 3791 advisers are about 33% of the 11,622 SEC-registered advisers.

[191] In the Proposing Release, the SEC requested comment on the estimate that approximately 90% of all financial institutions and creditors maintain covered accounts; the SEC received no comments on this estimate. *See supra* note 188 and accompanying text. If a financial institution or creditor does not maintain covered accounts, there will be no ongoing annual burden for purposes of the PRA.

[192] This estimate is based on the following calculation: 9305 financial institutions and creditors that maintain covered accounts × 8 hours = 74,440 hours.

[193] This estimate is based on the following calculation: 20,678 hours (10,339 financial institutions and creditors × 2 hours (for review of accounts)) + 55,830 hours (9305 financial institutions and creditors that maintain covered accounts × 6 hours (for report to board, and review and update of Program)) = 76,508 hours.

[194] § 248.202(a).

[195] *See* 5 U.S.C. 601–612.

[196] 47 FR 18618 (Apr. 30, 1982).

[197] *See* 75 FR 81519 (Dec. 28, 2010); 76 FR 6708 (Feb. 8, 2011); 76 FR 6715 (Feb. 8, 2011).

[198] *See, e.g.*, 75 FR 81519 (Dec. 28, 2010).

are expected to comprise the largest global financial institutions—and the CFTC is required to exempt from designation as an SD entities that engage in a de minimis level of swaps dealing in connection with transactions with or on behalf of customers. Accordingly, for purposes of the RFA, the CFTC has determined that SDs not be considered ''small entities'' for essentially the same reasons that it has previously determined FCMs not to be small entities.[199]

The CFTC also has previously determined that large traders are not ''small entities'' for RFA purposes, with the CFTC considering the size of a trader's position to be the only appropriate test for the purpose of large trader reporting.[200] The CFTC also has noted that MSPs maintain substantial positions in swaps, creating substantial counterparty exposure that could have serious adverse effects on the financial stability of the United States banking system or financial markets.[201] Accordingly, for purposes of the RFA, the CFTC has determined that MSPs not be considered ''small entities'' for essentially the same reasons that it has previously determined large traders not to be small entities.[202]

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

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

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

[199] *Id.*

[200] *See* 47 FR 18618 (Apr. 30, 1982).

[201] *See, e.g.*, 75 FR 81519 (Dec. 28, 2010).

[202] *Id.*

[203] *See, e.g.*, 77 FR 2613 (Jan. 19, 2012); 77 FR 20128 (Apr. 3, 2012).

SEC

The SEC has prepared the following Final Regulatory Flexibility Analysis (''FRFA'') regarding Regulation S–ID in accordance with 5 U.S.C. 604. The SEC included an Initial Regulatory Flexibility Analysis (''IRFA'') in the Proposing Release in February 2012.[204]

1. Need for Regulation S–ID

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

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

2. Significant Issues Raised by Public Comment

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

3. Small Entities Subject to the Rule

For purposes of the Regulatory Flexibility Act (''RFA''), an investment company is a small entity if it, together with other investment companies in the same group of related investment companies, has net assets of $50 million or less as of the end of its most recent fiscal year. SEC staff estimates that approximately 119 of the 1692 active open-end investment companies registered on Form N–1A meet this definition.[205]

[204] *See* Proposing Release, *supra* note 12.

[205] 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.

Under SEC rules, for purposes of the Investment 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.[206] Based on information in filings submitted to the SEC, 561 of the approximately 11,622 investment advisers registered with the SEC are small entities.[207]

For purposes of the RFA, a broker-dealer is a small business if it had total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to rule 17a–5(d) of the Exchange Act or, if not required to file such statements, a broker-dealer that had total capital (net worth plus subordinated liabilities) of less than $500,000 on the last business day of the preceding fiscal year (or in the time that it has been in business, if shorter) and if it is not an affiliate of an entity that is not a small business.[208] SEC staff estimates that approximately 797 broker-dealers meet this definition.[209]

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements

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

[206] 17 CFR 275.0–7(a).

[207] This information is based on data from the Investment Adviser Registration Depository (IARD) as of July 1, 2012.

[208] 17 CFR 240.0–10(c).

[209] This estimate is based on information provided in FOCUS Reports filed with the SEC as of July 1, 2012. There are approximately 4706 broker-dealers registered with the SEC.

mitigates the risk of identity theft applicable to these accounts.

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

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

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

5. Agency Action To Minimize Effect on Small Entities

The RFA directs the SEC to consider significant alternatives that would accomplish our stated objective, while minimizing any significant economic impact on small issuers. In connection with Regulation S–ID, the SEC considered the following alternatives: (i) The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (ii) the clarification, consolidation, or simplification of compliance requirements under Regulation S–ID for small entities; (iii) the use of performance rather than design standards; and (iv) an exemption from coverage of Regulation S–ID, or any part thereof, for small entities.

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

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

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

IV. Statutory Authority and Text of Amendments

The CFTC is amending Part 162 under the authority set forth in sections 1088(a)(8), 1088(a)(10), and 1088(b) of the Dodd-Frank Act,[211] and sections 615(e), 621(b), 624, and 628 of the FCRA.[212]

The SEC is adopting Regulation S–ID under the authority set forth in sections 1088(a)(8), 1088(a)(10), and 1088(b) of the Dodd-Frank Act,[213] section 615(e) of the FCRA,[214] sections 17 and 23 of the Exchange Act,[215] sections 31 and 38 of the Investment Company Act,[216] and sections 204 and 211 of the Investment Advisers Act.[217]

List of Subjects

17 CFR Part 162

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

17 CFR Part 248

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

Text of Final Rules

Commodity Futures Trading Commission

For the reasons stated above in the preamble, the Commodity Futures

[210] *See supra* note 8.

[211] Pub. L. 111–203, §§ 1088(a)(8), 1088(a)(10), and § 1088(b), 124 Stat. 1376 (2010).

[212] 15 U.S.C 1681–(e), 1681s(b), 1681s–3 and note, and 1681w(a)(1).

[213] Pub. L. 111–203, §§ 1088(a)(8), 1088(a)(10), 1088(b), 124 Stat. 1376 (2010).

[214] 15 U.S.C. 1681m(e).

[215] 15 U.S.C. 78q and 78w.

[216] 15 U.S.C. 80a–30 and 80a–37.

[217] 15 U.S.C. 80b–4 and 80b–11.

Trading Commission is amending 17 CFR part 162 as follows:

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

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

Authority: Sec. 1088, Pub. L. 111–203; 124 Stat. 1376 (2010).

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

Subpart C—Identity Theft Red Flags

Sec.

Subpart C—Identity Theft Red Flags

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

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

(b) *Special definitions for this subpart.* For purposes of this section, and Appendix B to this part, the following definitions apply:

(1) Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes an extension of credit, such as the purchase of property or services involving a deferred payment.

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

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated senior management employee.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a margin account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning in Sec. 603(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) 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.

(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.

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

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

Section 162.30 requires each financial institution or creditor that offers or maintains one or more covered accounts, as defined in § 162.30(b)(3), to develop and provide for the continued administration of a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of an Identity Theft Prevention Program that satisfies the requirements of § 162.30.

I. The Identity Theft Prevention Program

In designing its Identity Theft Prevention Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

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

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

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

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

(4) Its previous experiences with identity theft.

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

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

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

(3) Applicable supervisory guidance.

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

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

(2) The presentation of suspicious documents;

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

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

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

III. Detecting Red Flags

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

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and

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

IV. Preventing and Mitigating Identity Theft

The Identity Theft Prevention Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution or creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Internet Web site. Appropriate responses may include the following:

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

(b) Contacting the customer;

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

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

(e) Not opening a new covered account;

(f) Closing an existing covered account;

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

(h) Notifying law enforcement; or

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

V. Updating the Identity Theft Prevention Program

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

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; 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.

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

PART 248—REGULATIONS S–P, S–AM, AND S–ID

■ 4. 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, 78mm, 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, secs. 1088(a)(8), (a)(10), and sec. 1088(b), 124 Stat. 1376 (2010).

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

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

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

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

(ii) In the case of a financial institution or creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681m(e)(4).

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identifying information* means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

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

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

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

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

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

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

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

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

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

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

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

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

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

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

(4) Its previous experiences with identity theft.

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

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

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

(3) Applicable regulatory guidance.

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

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

(2) The presentation of suspicious documents;

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

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

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

III. Detecting Red Flags

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

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

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

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site. Appropriate responses may include the following:

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

(b) Contacting the customer;

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

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

(e) Not opening a new covered account;

(f) Closing an existing covered account;

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

(h) Notifying law enforcement; or

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

V. Updating the Program

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

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

(b) Changes in methods of identity theft;

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

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

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

VI. Methods for Administering the Program

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

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

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

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

(b) *Reports.*

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

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

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

VII. Other Applicable Legal Requirements

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

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

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

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

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

Supplement A to Appendix A

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

Alerts, Notifications or Warnings From a Consumer Reporting Agency

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

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

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

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

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

b. An unusual number of recently established credit relationships;

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

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

Suspicious Documents

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

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

7. Other information on the identification is not consistent with information provided

by the person opening a new covered account or customer presenting the identification.

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

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

Suspicious Personal Identifying Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dated: April 10, 2013.

By the Commodity Futures Trading Commission.

Melissa Jurgens,

Secretary of the Commodity Futures Trading Commission.

Dated: April 10, 2013

By the Securities and Exchange Commission.

Elizabeth M. Murphy,

Secretary of the Securities and Exchange Commission.

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

BILLING CODE 6351–01–P; 8011–01–p

Interagency Guidelines Establishing Information Security Standards

federalreserve.gov

I. Introduction

Purpose and Scope of the Guide

This Small-Entity Compliance Guide[1] is intended to help financial institutions[2] comply with the Interagency Guidelines Establishing Information Security Standards (Security Guidelines).[3] The guide summarizes the obligations of financial institutions to protect customer information and illustrates how certain provisions of the Security Guidelines apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs.

Although this guide was designed to help financial institutions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, this guide only addresses obligations of financial institutions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting customer records and information.

Background and Overview of Security Guidelines

The Security Guidelines implement section 501(b) of the Gramm-Leach-Bliley Act (GLB Act)[4] and section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[5] The Security Guidelines establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information.

Each of the requirements in the Security Guidelines regarding the proper disposal of customer information also apply to personal information a financial institution obtains about individuals regardless of whether they are the institution's customers ("consumer information"). Consumer information includes, for example, a credit report about: (1) an individual who applies for but does not obtain a loan; (2) an individual who guaantees a loan; (3) an employee; or (4) a prospective employee. A financial institution must require, by contract, its service providers that have access to consumer information to develop appropriate measures for the proper disposal of the information.

Under the Security Guidelines, each financial institution must:

- Develop and maintain an effective information security program tailored to the complexity of its operations, and
- Require, by contract, service providers that have access to its customer information to take appropriate steps to protect the security and confidentiality of this information.

The standards set forth in the Security Guidelines are consistent with the principles the Agencies follow when examining the security programs of financial institutions.[6] Each financial institution must identify and evaluate risks to its customer information, develop a plan to mitigate the risks, implement the plan, test the plan, and update the plan when necessary. If an Agency finds that a financial institution's performance is deficient under the Security Guidelines, the Agency may take action, such as requiring that the institution file a compliance plan.[7]

Distinction between the Security Guidelines and the Privacy Rule

The requirements of the Security Guidelines and the interagency regulations regarding financial privacy (Privacy Rule)8 both relate to the confidentiality of customer information. However, they differ in the following key respects:

- The Security Guidelines address safeguarding the confidentiality and security of customer information and ensuring the proper disposal of customer information. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access or use of, that information. The Security Guidelines provide that financial institutions must contractually require their affiliated and non-affiliated third party service providers that have access to the financial institution's customer information to protect that information.
- The Privacy Rule limits a financial institution's disclosure of nonpublic personal information to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's nonpublic personal information to a nonaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure.9 The Privacy Rule requires that privacy notices provided to customers and consumers describe the financial institution's

policies and practices to protect the confidentiality and security of that information. It does not impose any other obligations with respect to safeguarding customers' or consumers' information.

II. Important Terms Used in the Security Guidelines

Customer Information
The Security Guidelines require financial institutions to safeguard and properly dispose of customer information. Customer information is any record containing nonpublic personal information about an individual who has obtained a financial product or service from the institution that is to be used primarily for personal, family, or household purposes and who has an ongoing relationship with the institution.

Customer Information Systems
Customer information systems means any method used to access, collect, store, use, transmit, protect, or dispose of customer information. ¶I.C.2 of the Security Guidelines. Customer information systems encompass all the physical facilities and electronic facilities a financial institution uses to access, collect, store, use, transmit, protect, or dispose of customer information. The Security Guidelines apply specifically to customer information systems because customer information will be at risk if one or more of the components of these systems are compromised.

Information Security Program
An information security program is the written plan created and implemented by a financial institution to identify and control risks to customer information and customer information systems and to properly dispose of customer information. The plan includes policies and procedures regarding the institution's risk assessment, controls, testing, service-provider oversight, periodic review and updating, and reporting to its board of directors.

Service Providers
Service provider means any party, whether affiliated or not, that is permitted access to a financial institution's customer information through the provision of services directly to the institution. ¶I.C.2 of the Security Guidelines.

For example, a processor that directly obtains, processes, stores, or transmits customer information on an institution's behalf is its service provider. Similarly, an attorney, accountant, or consultant who performs services for a financial institution and has access to customer information is a service provider for the institution.

III. Developing and Implementing an Information Security Program

Paragraphs II.A-B of the Security Guidelines require financial institutions to implement an information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives:

- Ensure the security and confidentiality of their customer information;
- Protect against any anticipated threats or hazards to the security or integrity of their customer information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
- Ensure the proper disposal of customer information.

To achieve these objectives, an information security program must suit the size and complexity of a financial institution's operations and the nature and scope of its activities.

The various business units or divisions of the institution are not required to create and implement the same policies and procedures. If the business units have different security controls, the institution must include them in its written information security program and coordinate the implementation of the controls to safeguard and ensure the proper disposal of customer information throughout the institution.

Implementing an information security program begins with conducting an assessment of reasonably foreseeable risks. Like other elements of an information security program, risk assessment procedures, analysis, and results must be written.

Under the Security Guidelines, a risk assessment must include the following four steps:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
- Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the customer information;

- Assessing the sufficiency of the policies, procedures, customer information systems, and other arrangements in place to control the identified risks; and
- Applying each of the foregoing steps in connection with the disposal of customer information.

Identifying reasonably foreseeable internal and external threats

A risk assessment must be sufficient in scope to identify the reasonably foreseeable threats from within and outside a financial institution's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, as well as the reasonably foreseeable threats due to the disposal of customer information. The scale and complexity of its operations and the scope and nature of an institution's activities will affect the nature of the threats an institution will face.

For example, a financial institution should review the structure of its computer network to determine how its computers are accessible from outside the institution. If the computer systems are connected to the Internet or any outside party, an institution's assessment should address the reasonably foreseeable threats posed by that connectivity.

The risk assessment also should address the reasonably foreseeable risks to:

- Customer information stored on systems owned or managed by service providers, and
- Customer information disposed of by the institution's service providers.

Assessing the likelihood and potential damage of identified threats

In addition to identifying reasonably foreseeable threats to customer information, customer information systems, and customer information that a financial institution disposes of, a risk assessment must evaluate the potential damage from these threats. The Security Guidelines allow latitude to determine the sensitivity of customer information in the course of assessing the likelihood of and potential damage from the identified threats.

For example, to determine the sensitivity of customer information, an institution could develop a framework that analyzes the relative value of this information to its customers based on whether improper access to or loss of the information would result in harm or inconvenience to them.

In the course of assessing the potential threats identified, an institution should consider its ability to identify unauthorized changes to customer records. In addition, it should take into consideration its ability to reconstruct the records from duplicate records or backup information systems.

Assessing the sufficiency of policies and procedures

Evaluating the sufficiency of policies and procedures is a key element of a financial institution's risk assessment. The evaluation process includes identifying weaknesses or other deficiencies in existing security controls and assessing the extent to which customer information and customer information systems are at risk as a result of those weaknesses. It should also identify the extent to which customer information is at risk as a result of improper methods of disposal.

The risk assessment may include an automated analysis of the vulnerability of certain customer information systems. However, an automated analysis likely will not address manual processes and controls, detection of and response to intrusions into information systems, physical security, employee training, and other key controls. Accordingly, an automated analysis of vulnerabilities should be only one tool used in conducting a risk assessment.

When performing a risk assessment, an institution may want to consult the resources and standards listed in the appendix to this guide and consider incorporating the practices developed by the listed organizations when developing its information security program.[10]

Hiring an outside consultant to conduct the risk assessment

A financial institution may decide to hire an outside consultant to conduct the risk assessment of its information security program, but it nevertheless remains responsible for the adequacy of the assessment. Therefore, the institution must ensure that the assessment specifically examines the risks that relate to its customer information, customer information systems, and systems for disposal of customer information.

For example, a generic assessment that describes vulnerabilities commonly associated with the various

systems and applications used by the institution is inadequate. The assessment should take into account the particular configuration of the institution's systems and the nature of its business.

If an outside consultant only examines a subset of the institution's risks, such as risks to computer systems, that is insufficient to meet the requirement of the Security Guidelines. The institution will need to supplement the outside consultant's assessment by examining other risks, such as risks to customer records maintained in paper form.

For example, a financial institution should also evaluate the physical controls put into place, such as the security of customer information in cabinets and vaults.

Management must review the risk assessment and use that assessment as an integral component of its information security program to guide the development of, or adjustments to, the institution's information security program.

Engaging in an ongoing risk assessment process
Risk assessment is an ongoing process. Financial institutions should continually review their current policies and procedures to make certain they are adequate to safeguard customer information and customer information systems. The review of policies and procedures should also ensure the proper disposal of customer information. Financial institutions should also include their review and findings in their written information security program. The institution must also update the risk assessment, as necessary, to account for system changes before they are implemented, or new products or services before they are offered.

IV. Designing Security Controls

The Security Guidelines require a financial institution to design an information security program to control the risks identified through its assessment, commensurate with the sensitivity of the information and the complexity and scope of its activities. Thus, an institution must consider a variety of policies, procedures, and technical controls and adopt those measures that it determines appropriately address the identified risks.

The Security Guidelines provide a list of measures that an institution must consider and, if appropriate, adopt. These are:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program;
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
- Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

¶III.C.1.a-h of the Security Guidelines.

For example, the Security Guidelines require a financial institution to consider whether it should adopt controls to authenticate and permit only authorized individuals access to certain forms of customer information. ¶III.C.1.a of the Security Guidelines. Under this security control, a financial institution also should consider the need for a firewall for electronic records. If an institution maintains any sort of Internet or other external connectivity, its systems may require multiple firewalls with adequate capacity, proper placement, and appropriate configurations.

Similarly, an institution must consider whether the risk assessment warrants encryption of electronic customer information. If it does, the institution must

adopt appropriate encryption measures that protect information in transit, in storage, or both. ¶III.C.1.c of the Security Guidelines. However, the Security Guidelines do not impose any specific authentication[11] or encryption standards.[12]

A financial institution must consider the use of an intrusion detection system to alert it to attacks on computer systems that store customer information. ¶III.C.1.f. of the Security Guidelines. In assessing the need for such a system, an institution should evaluate the ability of its staff to rapidly and accurately identify an intrusion. It should also assess the damage that could occur between the time an intrusion occurs and the time the intrusion is recognized and action is taken.

Financial institutions must develop, implement, and maintain appropriate measures to properly dispose of customer information in accordance with each of the requirements of paragraph III. ¶III.C.4. of the Security Guidelines. Although the Security Guidelines do not prescribe a specific method of disposal, the Agencies expect institutions to have appropriate risk-based disposal procedures for their records.

An institution should:

- Ensure that paper records containing customer information are rendered unreadable as indicated by its risk assessment, such as by shredding or any other means; and
- Recognize that computer-based records present unique disposal problems. Residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive electronic data.

In addition to considering the measures required by the Security Guidelines, each institution may need to implement additional procedures or controls specific to the nature of its operations. An institution may implement safeguards designed to provide the same level of protection to all customer information, provided that the level is appropriate for the most sensitive classes of information.

Insurance coverage is not a substitute for an information security program. Although insurance may protect an institution or its customers against certain losses associated with unauthorized disclosure, misuse, alteration, or destruction of customer information, the Security Guidelines require a financial institution to implement and maintain controls designed to prevent those acts from occurring.

Develop and Implement A Response Program

The Agencies have issued an interpretation of the Security Guidelines regarding programs to respond to unauthorized access to customer information, the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Incident Response Guidance).[13] According to the Incident Response Guidance a financial institution should develop and implement a response program as part of its information security program. The response program should address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused;
- Prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information;
- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention;
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence; and
- Notification to customers when warranted.

Circumstances for Customer Notice

The Incident Response Guidance describes when and how a financial institution should provide notice to customers affected by unauthorized access or misuse of sensitive customer information. In particular, it indicates that:

- Once the institution becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused.
- If the institution determines that misuse of customer information has occurred or is reasonably possible, it should notify any affected customer as soon as possible.[14]

Sensitive customer information means:

- A customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account; or
- Any combination of components of customer information that would allow an unauthorized third party to access the customer's account electronically, such as user name and password or password and account number.

V. Training Staff

The Security Guidelines require a financial institution to train staff to prepare and implement its information security program. ¶III.C.2 of the Security Guidelines. The institution should consider providing specialized training to ensure that personnel sufficiently protect customer information in accordance with its information security program.

For example, an institution should:

- Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling;[15]
- Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and
- Train staff to properly dispose of customer information.

VI. Testing Key Controls

The Security Guidelines require a financial institution to test the key controls, systems, and procedures of its information security program. ¶III.C.3 of the Security Guidelines. The institution's risk assessment should determine the scope, sequence, and frequency of testing.

The Agencies expect an institution or its consultant to regularly test key controls at a frequency that takes into account the rapid evolution of threats to computer security. Testing may vary over time depending, in part, on the adequacy of any improvements an institution implements to prevent access after detecting an intrusion. Independent third parties or staff members, other than those who develop or maintain the institution's security programs, must perform or review the testing.

VII. Overseeing Service Providers

The Security Guidelines set forth specific requirements that apply to a financial institution's arrangements with service providers. An institution must:

- Exercise appropriate due diligence in selecting its service providers;
- Require its service providers by contract to implement appropriate measures designed to meet the objectives of the Security Guidelines; and
- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

As stated in section II of this guide, a service provider is any party that is permitted access to a financial institution's customer information through the provision of services directly to the institution. Examples of service providers include a person or corporation that tests computer systems or processes customers' transactions on the institution's behalf, document-shredding firms, transactional Internet banking service providers, and computer network management firms.

Contracts with Service Providers

The contract provisions in the Security Guidelines apply to all of a financial institution's service providers. After exercising due diligence in selecting a company, the institution must enter into and enforce a contract with the company that requires it to implement appropriate measures designed to implement the objectives of the Security Guidelines.[16]

In particular, financial institutions must require their service providers by contract to

- Implement appropriate measures designed to protect against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer; and
- Properly dispose of customer information.

In addition, the Incident Response Guidance states

that an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible following any such incident.

Monitoring Service Providers

A financial institution must monitor each of its service providers in accordance with its risk assessment. However, the Security Guidelines do not impose any specific requirements regarding the methods or frequency of monitoring service providers to ensure that they are fulfilling their contractual obligations. Some service providers are financial institutions that are subject to the Security Guidelines, or to other standards for safeguarding information promulgated by their primary regulator, and therefore may have implemented their own information security programs.

To the extent that monitoring is warranted, a financial institution must confirm that the service provider is fulfilling its obligations under its contract. Institutions may review audits, summaries of test results, or equivalent evaluations of a service provider's work. These audits, tests, or evaluations should be conducted by a qualified party independent of management and personnel responsible for the development or maintenance of the service provider's security program.

The reports of test results may contain proprietary information about the service provider's systems or they may include non-public personal information about customers of another financial institution. Under certain circumstances it may be appropriate for service providers to redact confidential and sensitive information from audit reports or test results before giving the institution a copy. Where this is the case, an institution should make sure that the information is sufficient for it to conduct an accurate review, that all material deficiencies have been or are being corrected, and that the reports or test results are timely and relevant.

The institution should include reviews of its service providers in its written information security program.

VIII. Adjusting the Program

A financial institution should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls necessary to safeguard customer information and ensure the proper disposal of customer information. It should adjust the program to take into account changes in technology, the sensitivity of its customer information, internal or external threats to information, and the institution's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

For example, the institution should ensure that its policies and procedures regarding the disposal of customer information are adequate if it decides to close or relocate offices. A change in business arrangements may involve disposal of a larger volume of records than in the normal course of business.

IX. Responsibilities of and Reports to the Board of the Directors

Under the Security Guidelines, a financial institution's board of directors, or an appropriate committee of the board, must satisfy specific requirements designed to ensure that the institution's information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible. At the outset, the board, or appropriate committee, must approve the written information security program. Thereafter, the board or appropriate committee must oversee the implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing management reports. ¶III.A of the Security Guidelines.

Correspondingly, management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and compliance with the Security Guidelines. The report should describe material matters relating to the program.

For example, whether an institution conducts its own risk assessment or hires another person to conduct it, management should report the results of that assessment to the board or an appropriate committee.

The Security Guidelines provide an illustrative list of other material matters that may be appropriate to include in the report, such as decisions about risk management and control, arrangements with service providers, results of testing, security breaches or violations and

management's responses, and recommendations for changes in an information security program. ¶III.F of the Security Guidelines.

Appendix

Note: This list of resources is intended to further assist financial institutions in complying with the Interagency Guidelines Establishing Information Security Standards. The listed organizations provide information on computer security, with a focus on risk-assessment methodologies and the design and implementation of computer security programs. Any mention of a commercial product is for information purposes only and does not imply a recommendation or endorsement by the Agencies.

Center for Internet Security (CIS) -- A nonprofit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations. CIS develops security benchmarks through a global consensus process. Its members include the American Institute of Certified Public Accountants (AICPA), Financial Management Service of the U.S. Department of the Treasury, and Institute for Security Technology Studies (Dartmouth College). http://www.cisecurity.org/

CERT Coordination Center -- A center for Internet security expertise operated by Carnegie Mellon University. CERT provides security-incident reports, vulnerability reports, security-evaluation tools, security modules, and information on business continuity planning, intrusion detection, and network security. It also offers training programs at Carnegie Mellon. CERT has developed an approach for self-directed evaluations of information security risk called Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). www.cert.org/octave/

Information Systems Audit and Control Association (ISACA) -- An association that develops IT auditing and control standards and administers the Certified Information Systems Auditor (CISA) designation. ISACA developed Control Objectives for Information and Related Technology (COBIT) as a standard for IT security and control practices that provides a reference framework for management, users, and IT audit, control, and security practitioners. www.isaca.org/cobit.htm

International Organization for Standardization (ISO) -- A network of national standards institutes from 140 countries. Published ISO/IEC 17799:2000, Code of Practice for Information Security Management. http://www.iso.org/ . Interested parties should also review the Common Criteria for Information Technology Security Evaluation.

Internet Security Alliance (ISA) -- A collaborative effort between Carnegie Mellon University's Software Engineering Institute, the university's CERT Coordination Center, and the Electronic Industries Alliance (a federation of trade associations). ISA provides access to information on threats and vulnerability, industry best practices, and developments in Internet security policy. http://www.isalliance.org/

Institute for Security Technology Studies (Dartmouth College) -- An institute that studies and develops technologies to be used in counter-terrorism efforts, especially in the areas of threat characterization and intelligence gathering, threat detection and interdiction, preparedness and protection, response, and recovery. The institute publishes a daily news summary titled Security in the News, offers on-line training courses, and publishes papers on such topics as firewalls and virus scanning. The web site includes worm-detection tools and analyses of system vulnerabilities. http://www.ists.dartmouth.edu/

National Institute of Standards and Technology (NIST) -- An agency within the U.S. Commerce Department's Technology Administration that develops and promotes measurements, standards, and technology to enhance productivity. NIST operates the Computer Security Resource Center, which is dedicated to improving information systems security by raising awareness of IT risks, researching vulnerabilities, and developing standards and tests to validate IT security. Four particularly helpful documents are: Special Publication 800-14,Generally Accepted Principles and Practices for Securing Information Technology Systems; Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems; Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems; Special Publication 800-30, Risk Management Guide for Information Technology Systems; and Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems. csrc.nist.gov. The web site provides links to a large number of academic, professional, and government sponsored web sites that provide additional information on computer or

system security.

National Security Agency (NSA) -- The National Security Agency/Central Security Service is America's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. The web site includes links to NSA research on various information security topics. http://www.nsa.gov/

1. The guide is issued in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, reprinted in 5 U.S.C.A. § 601, note (West Supp. 2004).
2. This guide applies to the following types of financial institutions: National banks, Federal branches and Federal agencies of foreign banks and any subsidiaries of these entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OCC); member banks (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, Edge and Agreement Act Corporations, bank holding companies and their nonbank subsidiaries or affiliates (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (Board); state non-member banks, insured state branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (FDIC); and insured savings associations and any subsidiaries of such savings associations (except brokers, dealers, persons providing insurance, investment companies, and investment advisers) (OTS).

3. 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). Citations to the Security Guidelines in this guide omit references to part numbers and give only the appropriate paragraph number.

4. 15 U.S.C. § 6801.

5. 15 U.S.C. § 1681w.

6. See Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet (the "IS Booklet").

7. 12 U.S.C. § 1831p-1. There are a number of other enforcement actions an agency may take. For example, the OTS may initiate an enforcement action for violating 12 C.F.R. § 568.5 based on noncompliance with the Security Guidelines.

8. Each of the Agencies, as well as the National Credit Union Administration (NCUA), has issued privacy regulations that implement sections 502-509 of the GLB Act; the regulations are comparable to and consistent with one another. See 65 Fed. Reg. 35,162 (June 1, 2000) (Board, FDIC, OCC, OTS) and 65 Fed. Reg. 31740 (May 18, 2000) (NCUA) promulgating 12 C.F.R. Parts 40 (OCC), 216 (Board), 332 (FDIC), 573 (OTS), and 716 (NCUA). Citations to the Privacy Rule in this guide omit references to part numbers and give only the appropriate section number.

9. The Privacy Rule defines a "consumer" to mean an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes. For example, an individual who applies to a financial institution for credit for personal purposes is a consumer of a financial service, regardless of whether the credit is extended. Privacy Rule § __.3(e).

10. Financial institutions also may want to consult the Agencies' guidance regarding risk assessments described in the IS Booklet.

11. On December 14, 2004, the FDIC published a study, Putting an End to Account-Hijacking Identity Theft (682 KB PDF), which discusses the use of authentication technologies to mitigate the risk of identity theft and account takeover. FDIC Financial Institution Letter (FIL) 132-2004. Additional discussion of authentication technologies is included in the FDIC's June 17, 2005, Study Supplement. FIL 59-2005.

12. The Agencies have issued guidance about authentication, through the FFIEC, entitled "Authentication in an Internet Banking Environment (163 KB PDF)" (Oct. 12, 2005). Additional information about encryption is in the IS Booklet.

13. 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS).

14. The Incident Response Guidance recognizes that customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

15. See "Identity Theft and Pretext Calling," FRB Sup. Ltr. SR 01-11 (April 26,2001) (Board); OCC Advisory Ltr. 2001-4 (April 30, 2001) (OCC); CEO Ltr. 139 (May 4, 2001) (OTS); FIL 39-2001 (May 9, 2001) (FDIC).

16. The third-party-contract requirements in the Privacy Rule are more limited than those in the Security Guidelines. When a financial institution relies on the "opt out" exception for service providers and joint marketing described in § __.13 of the Privacy Rule (as opposed to other exceptions), in order to disclose nonpublic personal information about a consumer to a nonaffiliated third party without first providing the consumer with an opportunity to opt out of that disclosure, it must enter into a contract with that third party. The contract must generally prohibit the nonaffiliated third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.

Fighting Fraud with the Red Flags Rule

ftc.gov

Are you complying with the Red Flags Rule?

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations. By identifying red flags in advance, businesses will be better equipped to spot suspicious patterns that may arise -- and take steps to prevent a red flag from escalating into a costly episode of identity theft.

Resources on this site can help business people educate their staff and colleagues about complying with the Red Flags Rule.

What Compliance Looks Like

Your Identity Theft Prevention Program is a "playbook" that must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. Your Program should enable your organization to:

1. identify relevant patterns, practices, and specific forms of activity — the "red flags" — that signal possible identity theft;
2. incorporate business practices to detect red flags;
3. detail your appropriate response to any red flags you detect to prevent and mitigate identity theft; and
4. be updated periodically to reflect changes in risks from identity theft.

The Red Flags Rule also includes guidelines to help financial institutions and creditors develop and implement a Program, including a supplement that offers examples of red flags.

The FTC and the federal financial agencies have issued Frequently Asked Questions and answers to help businesses comply with the Rule.

Who Must Comply with the Red Flags Rule?

The Rule requires "financial institutions" and "creditors" that hold consumer accounts designed to permit multiple payments or transactions -- or any other account for which there is a reasonably foreseeable risk of identity theft -- to develop and implement an Identity Theft Prevention Program for new and existing accounts. The definition of "financial institution" includes:

- all banks, savings associations, and credit unions, regardless of whether they hold a transaction account belonging to a consumer; and
- anyone else who directly or indirectly holds a transaction account belonging to a consumer.

A change in the law on December 18, 2010 amended the the definition of "creditor," and limits the circumstances under which creditors are covered. The new law covers creditors who regularly, and in the ordinary course of business, meet one of three general criteria. They must:

- obtain or use consumer reports in connection with a credit transaction;
- furnish information to consumer reporting agencies in connection with a credit transaction; or
- advance funds to -- or on behalf of -- someone, except for funds for expenses incidental to a service provided by the creditor to that person.

About John Speer

Member | Bass Berry & Sims | Memphis, TN

901.543.5919 | jspeer@bassberry.com
http://www.bassberry.com/jspeer/

Mr. Speer is a member of the firm's Litigation and Dispute Resolution Practice. He concentrates on representing and counseling clients in complex litigation and commercial disputes with an emphasis on representing financial institutions.

Financial Services: Mr. Speer represents financial service companies in courts in the southeast and other parts of the country and in negotiating disputes involving troubled commercial and real estate loans. He also represents clients in the financial services sector in matters involving investigations by regulators and other federal and state agencies.

Commercial: Representation of clients in general commercial litigation and in mediating and negotiating disputes in the healthcare, transportation, manufacturing and professional service industries is also a part of Mr. Speer's practice. He has represented clients in a variety of cases including stockholder derivative actions, dissenting shareholder class actions, and breach of trust and fiduciary duty cases involving officers and directors of public and private companies.

Honors and Distinctions

- Listed in: Best Lawyers®; Chambers USA; Mid-South Super Lawyers; MBQ: Inside Memphis Business Power Players
- Seminar Presenter: American Bankers Association; National Institute of Business; Tennessee Bankers Association; Corporate Counsel of America
- Order of the Coif
- Member, Kentucky Law Review, 1971-1972

Publications

- "Courts, Congress Will Ultimately Steer Consumer Financial Protection Bureau," Memphis Business Journal (June 8, 2012)
- "Wallace v. National Bank of Commerce Bank Service Fee Litigation," The Tennessee Bankers Magazine (1995)
- "Litigation Report: Intent to Deceive in Securities Litigation," Memphis Business Journal

Education

- University of Kentucky - J.D., 1972
- University of Kentucky - B.A., 1969