

Securities and Futures & Derivatives Alert

April 25, 2013

SECURITIES

SEC and CFTC Issue Identity Theft Red Flags Rules

I. Introduction

On April 10, 2013, the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) jointly issued final rules and guidelines requiring certain SEC and CFTC-regulated entities that offer or maintain “covered accounts” to establish programs to address risks of identity theft.¹ These new rules largely transfer enforcement authority from the Federal Trade Commission (FTC) to the SEC and CFTC, as required under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act). However, the final rules also provide additional guidance that may help entities that have not implemented identity theft programs to evaluate whether they are required to do so.

II. Background

The SEC and CFTC’s joint rulemaking is the result of a shift in regulatory responsibility required by the Dodd-Frank Act. The Fair Credit Reporting Act of 1970 (FCRA),² as amended in 2003, required several federal banking regulators and the FTC—not including the SEC or CFTC—to issue joint rules and guidelines regarding the detection, prevention and mitigation of identity theft.³ This group issued its rules in 2007.⁴ While the FCRA did not, at that point, require the SEC and CFTC to join this rulemaking, certain entities registered with the SEC and CFTC were nonetheless covered by the rules, subject to the enforcement authority of the FTC.⁵ The Dodd-Frank Act amended the FCRA and transferred to the SEC and CFTC rulemaking and enforcement authority for identity theft rules with respect to entities the agencies regulate.⁶

III. Summary of the Rules

The new SEC and CFTC rules are substantially similar to those issued by the FTC and banking regulators. Accordingly, entities that have already implemented identity theft programs under those rules will likely not see substantial changes in their compliance requirements. However, according to the Commissions, while the final rules do not impose the requirement to establish programs on entities that were not previously covered, the rules include guidance focused on entities regulated by the SEC and CFTC, which may assist regulated entities that have not implemented identity theft programs in their assessment of whether they are required to do so.⁷

¹ See Identity Theft Red Flag Rules, 78 Fed. Reg. 23638 (April 19, 2013).

² Pub. L. 91-508, 84 Stat. 1114 (1970), codified at 15 U.S.C. § 1681-1681x.

³ See Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 117 Stat. 1952 (2003).

⁴ See Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, 72. Fed. Reg. 63719 (Nov. 9, 2007).

⁵ See 78 Fed. Reg. at 23639.

⁶ See 15 U.S.C. § 1681m(e)(1).

⁷ See 78 Fed. Reg. at 23639.

A. Requirements

Entities covered by these rules must adopt and implement an identity-theft program. This program must include policies and procedures designed to:

- identify relevant types of identity theft red flags;
- detect the occurrence of red flags;
- respond appropriately to red flags; and
- periodically update the identity theft program.⁸

Each financial institution or creditor must consider the set of guidelines provided in the rules, and include in its identity theft program those guidelines that are relevant and appropriate.⁹ An entity must provide for the continued administration of the program, and must obtain approval of the initial program from either its board of directors or an appropriate committee of the board of directors.¹⁰ The board of directors, a committee thereof, or an employee at the level of senior management must be involved in the oversight, development, implementation and administration of the program, and staff must be trained as necessary for effective implementation.¹¹ An entity must also exercise appropriate and effective oversight of service provider arrangements.¹²

Additionally, the rules require entities that issue debit cards or credit cards to take certain precautionary actions when they receive a request for a new card soon after they receive a notification of a change of address for a consumer's account.¹³

B. Covered Entities and Accounts

A financial institution or creditor must implement an identity theft program if it offers or maintains "covered accounts."¹⁴ The applicable definitions of "financial institutions" and "creditors" are based on those in the FCRA, but both the SEC and CFTC have elaborated upon the entities under their jurisdiction to which the rules apply.

The definitions in the SEC's rules directly incorporate the definition of "financial institution" from 15 U.S.C. § 1681a(t),¹⁵ and the definition of "creditor" from 15 U.S.C. § 1681m(e)(4).¹⁶ However, the SEC rules will apply only to a financial institution or creditor that is (1) a broker, dealer, or other person 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 1940.¹⁷

The CFTC's definition of "financial institution" also incorporates the FCRA's, but also specifies that it 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."¹⁸ Similarly, the CFTC's definition of "creditor" also incorporates the definition from 15 U.S.C. § 1681m(e)(4), but specifies that it includes "any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool

⁸ 17 C.F.R. § 162.30(d)(2); 17 C.F.R. § 248.201(d)(2).

⁹ 17 C.F.R. § 162.30(f); 17 C.F.R. § 248.201(f).

¹⁰ 17 C.F.R. § 162.30(e); 17 C.F.R. § 248.201(e).

¹¹ 17 C.F.R. § 162.30(e); 17 C.F.R. § 248.201(e).

¹² 17 C.F.R. § 162.30(e); 17 C.F.R. § 248.201(e).

¹³ 7 C.F.R. § 162.32; 17 C.F.R. § 248.202.

¹⁴ 78 Fed. Reg. at 23644.

¹⁵ 17 C.F.R. § 248.201(b)(7).

¹⁶ 17 C.F.R. § 248.201(b)(5).

¹⁷ 17 C.F.R. § 248.201(a).

¹⁸ 17 C.F.R. § 162.30(b)(7).

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.”¹⁹

Under both sets of rules, a “covered account” includes one offered or maintained “primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions,” as well as any other account “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.”²⁰ The CFTC rules specify that such accounts will include, when held primarily for personal, family, or household purposes, a margin account; the SEC rules specify that they will include, when held primarily for personal, family, or household purposes, 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.²¹ Covered accounts can include any account, including those held not primarily for personal, family, or household purposes, for which there is a reasonably foreseeable risk due to identity theft.

Periodically, each financial institution or creditor must assess whether it maintains or offers any covered accounts. This risk-based assessment must take into consideration the methods the entity provides to open its accounts, the methods it provides to access its accounts, and its previous experience with identity theft.

A firm must undertake a multi-step analysis to determine whether it should implement an identity theft program. First, a firm must determine whether it is a “financial institution” or “creditor” under the relevant definition. Significantly, while the definition of financial institution is limited to entities that provide transaction accounts for individuals, the definition of creditor does not include a comparable limitation. Second, if it is a financial institution or creditor, a firm must assess whether it offers or maintains covered accounts. Notably, covered accounts can include accounts for both natural persons and business entities. So, while qualification as a “financial institution” requires holding transaction accounts for individuals, a financial institution must assess whether accounts for both natural persons and businesses are “covered accounts.”²² Similarly, creditors must assess whether accounts for both natural persons and businesses are “covered accounts.”

Please see the appendix for an overview outline of this analysis.

IV. Application to Specific Entities

Again, it is likely that these rules will not alter compliance requirements for entities that have developed and implemented an identity theft program under the previous rules. However, in light of the new rules and guidance, other entities could consider re-evaluating whether they should implement such a program.

A. Investment Advisers

The adopting release clarifies that certain investment advisers will fall within the meaning of “financial institution” and therefore will be subject to these rules. The following are examples of SEC-registered investment advisers that will be subject to the rules:

- An adviser that has authority to direct payments or transfers out of accounts of individual clients or investors in funds managed by the adviser to third parties.²³
- An adviser that acts as an agent on behalf of the individual clients or investors in funds managed by the adviser.²⁴

¹⁹ 17 C.F.R. § 162.30(b)(5).

²⁰ 17 C.F.R. § 162.30(b)(3); 17 C.F.R. § 248.201(b)(3).

²¹ 17 C.F.R. § 162.30(b)(3); 17 C.F.R. § 248.201(b)(3).

²² 78 Fed. Reg. at 23644, n. 77.

²³ 78 Fed. Reg. at 23642.

²⁴ *Id.*

The guidance makes clear that an adviser authorized 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 paying third parties.²⁵ However, advisers authorized to withdraw investor funds and pay third parties would hold a transaction account.²⁶ This group can include registered investment advisers to private funds.²⁷

In addition, an adviser could fall within the definition of "creditor" and therefore be subject to these rules, if for example, the adviser advances capital to its funds or accounts of an individual to bridge capital contributions or subscriptions.

B. Broker-Dealers

These rules should not create new compliance requirements for broker-dealers, which have likely developed and implemented identity theft red flags programs under the previous rules. Broker-dealers should note, though, that as rules under the Exchange Act, the SEC's new identity theft program rules can be enforced by the Financial Industry Regulatory Authority (FINRA). FINRA previously consulted with the FTC on interpretive issues affecting broker-dealers under the previous rules for identity theft programs,²⁸ but did not have examination or enforcement authority.

C. Entities Regulated by the CFTC

As stated above, these rules also should not create new compliance requirements for CFTC-regulated entities. However, violations of the Commodity Exchange Act (CEA) may also subject a person to CFTC-specific criminal and civil penalties. Further, other sections of the CEA may now be invoked with respect to violations of the rules.

A violation of this rule may create a private right of action under the CEA. Section 22 of the CEA provides for a private right of action against any person who violates the CEA or who willfully aids, abets, counsels, induces or procures the commission of a violation of the CEA.

There are also potential issues of secondary liability in connection with a violation of these rules. Section 13(a) of the CEA imposes liability on any person that willfully aids, abets, commands, induces or procures the commission of a violation of any provision of the CEA. An aiding and abetting violation under the CEA requires proof of the same elements that are found in criminal or tort law. To be liable for aiding and abetting, the person must: (1) have knowledge of the intent to violate the CEA, (2) have intent to further that violation, and (3) commit an act in furtherance of the violation. Additionally, Section 13(b) provides that any person who directly or indirectly controls any person who has violated any provision of the CEA or Commission rule thereunder violates the CEA to the same extent as the controlled person. Any person that is associated with a violation of these rules would now be subject to these forms of secondary liability.

The rule change also shifts the enforcement authority over violations of these rules to the CFTC's Division of Enforcement. To the extent that the CFTC's Division of Enforcement more actively monitors and has greater familiarity with the entities subject to these rules, adherence to the rule may be subject to enhanced scrutiny.

Finally, the CFTC may delegate examination for compliance with this rule to the National Futures Association, which would subject CFTC-regulated entities to further supervision and possible regulatory penalties for non-compliance.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ See, e.g., FINRA Regulatory Notice 08-69 (Nov. 2008); see also FINRA's "Red Flag Rule" webpage, at: <http://www.finra.org/Industry/Issues/CustomerInformationProtection/p118480>.

V. Effective and Compliance Dates

The new rules will be effective 30 days after publication in the Federal Register, and the compliance date will be six months following the effective date.²⁹ Accordingly, the rules will be effective on May 19, 2013, and the compliance date will be November 19, 2013.

Appendix: Overview of Analysis for Applicability of Rules

1. Is the entity a “financial institution” or “creditor”?
 - a. Is it a “financial institution”?
 - i. 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...
 - ii. That, directly or indirectly, holds a transaction account³⁰ belonging to a consumer.
 - iii. For entities under the jurisdiction of the CFTC, “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.
 - b. Is it a “creditor”?
 - i. An entity that meets the definition under 15 U.S.C. § 1681m(e)(4).
 - ii. For entities under the jurisdiction of the CFTC, “creditor” 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.
2. If it is a financial institution or creditor under the SEC’s jurisdiction, is the entity...
 - a. A broker, dealer, or other person registered, or required to be registered, under the Securities Exchange Act of 1934;
 - b. 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
 - c. An investment adviser that is registered, or required to be registered, under the Investment Advisers Act of 1940?
3. If it is a covered financial institution or creditor, does the entity maintain or offer a “covered account”?
 - a. Is an account offered or maintained primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions?
 - i. For example, for SEC-regulated entities, 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.

²⁹ 78 Fed. Reg. at 23638.

³⁰ For the applicable definition of a “transaction account,” see 12 U.S.C. § 461(b)(1)(C).

- ii. For example, for CFTC-regulated entities, a margin account.
- b. Or, for any other accounts offered or maintained, is there a reasonably foreseeable risk to customers or to the safety and soundness of the entity from identity theft, including financial, operational, compliance, reputation, or litigation risks?

FOR MORE INFORMATION ON THIS OR OTHER SECURITIES AND FUTURES & DERIVATIVES MATTERS,
CONTACT:

Bruce H. Newman +1 212 230 8835 bruce.newman@wilmerhale.com
Timothy F. Silva +1 617 526 6502 timothy.silva@wilmerhale.com
Heather Zachary +1 202 663 6987 heather.zachary@wilmerhale.com
Zachary J. King +1 202 663 6149 zachary.king@wilmerhale.com
Alexander M. Jadin +1 202 663 6545 alex.jadin@wilmerhale.com

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 1875 Pennsylvania Avenue, NW, Washington, DC 20006, +1 202 663 6000. Our United Kingdom offices are operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK offices. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. ©2013 Wilmer Cutler Pickering Hale and Dorr LLP