MINTZ

SEC and CFTC Issue Final Joint Rules on "Red Flags" Compliance

April 24, 2013 | Alert | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

The Securities Exchange Commission ("SEC") and the Commodity and Futures Trade Commission ("CFTC") (together, the "Commissions") have issued **final joint rules and guidelines** that require certain entities regulated by the Commissions to establish programs to address risks of identity theft. The final joint rules are similar to the identity theft red flag rules ("Red Flag Rules") that were jointly issued by the Federal Trade Commission ("FTC") and other federal agencies in 2007, and the proposed joint rules that the Commissions issued in early 2012. The final joint rules implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, as amended ("Dodd-Frank"). Generally speaking, this means that entities like broker-dealers and federally registered investment advisers who were not covered under the earlier Red Flag Rules must now establish identity theft programs that comply with the new regulations.

For a brief overview of the SEC's comments related to the issuance of the joint rules, see an earlier blog post here.

Who must comply?

The joint rules apply to "financial institutions" and "creditors" that maintain a "covered account" and are subject to the Commissions' respective enforcement authorities. The joint rules do not specifically exclude any entities registered with the Commissions from their scope. Notably, the Commissions suggest that the entities whose activities fall within the joint rules are already covered by parallel red flags rules adopted by other federal agencies, and that their joint rules do not broaden the scope of entities or activities that are covered under the other federal agencies' red flags rules. The joint rules do, however, contain examples and minor language changes that could lead entities to determine that the joint rules apply to them, even though they previously may have determined that the other federal agencies' red flags rules did not apply.

> ***Practice Tip*: Even if an entity has previously determined that the other federal agencies' existing red flags rules do not apply to it, the entity should review the Commissions' final joint rules to determine if the examples and clarifications change its analysis.**

CFTC Scope

The CFTC defines "financial institution," as cross-referenced from Section 603(t) of the Fair Credit Reporting Act ("FCRA"), 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**).

In addition to the broader definition of financial institution, the CFTC lists the following specific entities that, when they directly or indirectly hold a transaction account belonging to a consumer, are deemed "financial institutions" under the joint rules:

- Futures Commission Merchant
- Retail Foreign Exchange Dealer
- Commodity Trading Advisor
- Commodity Pool Operator
- Introducing Broker

- Swap Dealer
- Major Swap Participant

Likewise, the CFTC applies the definition of "creditor" under the FCRA (**15 U.S.C. 1681m(e)(4)**) to any of the entities listed above 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." The CFTC explains that the 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 consumers or to the safety and soundness of the financial institution, from identity theft.

The definition of "covered account" under the joint rules is the same for both the CFTC and SEC, and is defined as:

- 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
- 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.

The CFTC's definition also includes a margin account as an example of a covered account.

SEC Scope

The SEC takes a simpler approach and provides that the joint rules apply to "financial institutions" and "creditors," as defined by the FCRA, that are one of the following:

- a broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934;
- an investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act; or
- an investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.

The SEC cautions that although some types of entities are not specifically named because they are *less likely* to qualify as financial institutions or creditors (such as nationally recognized statistical rating organizations, self-regulatory organizations, municipal advisors and municipal securities dealers), these entities nevertheless fall within the scope of the rules if they qualify as financial institutions or creditors.

In addition to the definition of "covered account" listed above under "CFTC Scope," the SEC definition includes, as examples of covered accounts, 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.

What is required?

Once an entity concludes that the joint rules apply, the next step is to determine what is required to comply. The joint rules establish four elements that are required for the entity's written identity theft prevention program (a "Program"), and those elements are further expanded in the Commissions' guidelines.

The Elements

A Program is required to have reasonable policies and procedures that do the following:

1. Identify red flags for covered accounts and incorporate those red flags into the Program.
2. Detect the red flags that the Program incorporates.
3. Respond appropriately to any red flags that they detect.
4. Periodically update the Program to reflect changes in risks to customers and in the safety and soundness of the financial institution or creditor from identity theft.

The Guidelines

Aside from the basic required elements of a Program, the Commissions have established the following more detailed guidelines to better assist financial institutions and creditors in creating a Program:

Section I: Identity Theft Prevention Program

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

Section II: Identifying Relevant Red Flags

Financial institutions and creditors must consider several risk factors in identifying relevant red flags, which include the following:

- the types of covered accounts offered or maintained;
- the methods provided to open or access covered accounts; and
- their previous experiences with identity theft.

Some examples from which financial institutions or creditors should derive red flags are incidents of identity theft that the entity has experienced and methods of identity theft that it has identified that reflect changes in identity theft risks. The guidance also outlines 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
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information, such as a suspicious address change
- Unusual use of a covered account
- Notice from customers, victims of identity theft, law enforcement agencies or others regarding possible identity theft in connection with a covered account

Supplement A to the guidelines provides illustrative examples of the above red flags that financial institution or creditors may consider incorporating into their Programs.

Section III: Detecting Red Flags

The Commissions provide some examples of policies and procedures for detecting red flags, such as by (i) obtaining identifying information about, and verifying the identify of, a person opening a covered account; and (ii) authenticating customers, monitoring transactions, and verifying the validity of change of address requests for covered accounts.

Section IV: Preventing and Mitigating Identity Theft

To prevent and mitigate identify theft, a Program's policies and procedures should provide for appropriate responses to the red flags that have been detected that are on par with the degree of risk posed by such red flags. To determine what constitutes an appropriate response, the financial institution or creditor must consider aggravating factors that may heighten the risk of identity theft. Appropriate responses may include:

- monitoring a covered account for evidence of identity theft;
- contacting the customer;
- changing passwords and security codes;
- closing an existing covered account; and
- notifying law enforcement.

Section V: Updating the Identity Theft Prevention Program

A financial institution or creditor should update its Program periodically, based on its experiences with identity theft, changes in methods of identity theft or methods to detect, prevent and mitigate identity theft, changes in the types of accounts offered or maintained, and changes in its business arrangements, including mergers, acquisitions and joint ventures.

Section VI: Methods for Administering the Identity Theft

The Program should be overseen by the entity's board of directors, a committee of the board of directors, or a designated senior management employee. This oversight should include assisting specific responsibility for the Program's implementation, reviewing reports prepared by staff regarding compliance by the entity, and approving material changes to the Program.

Section VII: Other Applicable Legal Requirements

This Commissions list additional legal requirements that may apply to specific circumstances, including when a financial institution or creditor detects a fraud or active duty alert, correcting or updating inaccurate or incomplete information to consumer reporting agencies, and prohibitions on the sale or transfer of the collection of certain debts.

What now?

The joint rules will become effective 30 days after publication in the Federal Register, and the compliance date will be six months after that effective date. During this time, entities regulated by the SEC or CFTC should assess whether the joint rules apply to them. This assessment should be done in the context of the examples provided by the Commissions in the joint rules, especially if an entity has previously determined that the red flags rules issued by the FTC and other federal agencies do not apply. Financial

institutions and creditors regulated by the Commissions should periodically reassess whether compliance is required due to changes in accounts offered or maintained, or otherwise due to changes in the entity's business.

* * *

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.