SEC AND CFTC ADOPT IDENTITY THEFT RED FLAG RULES

The Securities and Exchange Commission and the Commodity Futures Trading Commission have adopted new rules that require certain "financial institutions" and "creditors" that offer or maintain "covered accounts" to establish written identity theft red flag procedures designed to detect, prevent and mitigate identity theft.[1]

The compliance date for these rules is November 20, 2013.

Background

The obligation of SEC and CFTC regulated entities to mitigate the likelihood that their customers' personal information will be stolen is not new. The identity theft rules of other federal regulators already previously applied to such entities. In 2010, the Dodd-Frank Act transferred authority to the SEC and CFTC for entities that are subject to their respective authority.[2] The Release notes that the rules adopted do not contain any requirements that were not already in other federal agencies' rules.

SEC and CFTC Regulated Entities within the Scope of the Rules

SEC regulated entities covered by the rules include brokers, dealers, registered investment companies, business development companies, employee securities companies and registered investment advisers. CFTC regulated entities covered by the rules include futures commission merchants, retail foreign exchange dealers, commodity trading advisors, commodity pool operators, introducing brokers, swap dealers and major swap participants.

---

1 The new rules were issued by the SEC and CFTC on April 10, 2013 in a joint release entitled *Identity Theft Red Flags Rules* (the "Release"). *See* 17 CFR Part 162 and 17 CFR Part 248.

2 The Fair Credit Reporting Act of 1970 (the "FCRA") set standards for the collection, communication and use of information about consumers by consumer reporting agencies. *See* 18 U.S.C. § 1681 *et seq.* The FCRA was amended in 2003 by the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act"), which, among other things, directed certain federal agencies to issue rules and guidelines relating to identity theft. *See* Pub. L. 108-159, 117 Stat. 1952 (2003). Among the agencies directed to issue identity theft rules were the Federal Trade Commission, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the National Credit Union Administration. The Dodd-Frank Wall Street Reform and Consumer Protection Act amended the FCRA to add the SEC and the CFTC to the list of agencies required to issue and enforce identity theft rules. *See* Pub. L. 111-203, 124 Stat. 1376 (2010).

Financial Institutions and Creditors

An SEC or CFTC regulated entity would have to comply with the rules only if the entity also is a "financial institution" or a "creditor."

A "financial institution" is, generally, any person that, directly or indirectly, holds a "transaction account" belonging to a consumer. A "transaction account" is an account with respect to which a "consumer" is permitted to make withdrawals for the purpose of making payments or transfers to third parties. A "consumer" means an individual person.

Examples of SEC regulated entities that would be financial institutions subject to the rules include (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. The SEC clarified that an investment adviser may hold a transaction account when the adviser has the ability to direct transfers or payments (e.g., redemptions, distributions, dividends or interest) from accounts belonging to an individual to third parties at the individual's instruction. On the other hand, an adviser who has authority to withdraw money from an individual's account only in order to pay the adviser's fee, would not be deemed to hold a transaction account.

CFTC regulated entities that may be financial institutions include: any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer or major swap participant, that directly or indirectly holds a transaction account belonging to a customer.

Under the rules, a "creditor" is, generally, a person that extends credit or lends funds to or on behalf of a person that is obligated to repay the loan. In addition to certain brokers or dealers that may meet the definition of creditor, the Release states that an investment adviser could be a creditor if the adviser "advances funds" to an investor. By way of example, the Release states that a private fund adviser could be a creditor if the adviser regularly and in the ordinary course of business lends money, short-term or otherwise, to a prospective investor, pending receipt or clearance of the investor's check or wire transfer. A private fund adviser would not, however, be a creditor solely because its private funds regularly borrow money from third-party credit facilities pending receipt of investor subscriptions, as the definition of "creditor" does not include "indirect" creditors.

The CFTC's definition of "creditor" includes any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer and major swap participant, that regularly extends, renews or continues credit or makes those arrangements.

Covered Accounts

An SEC or CFTC regulated entity that meets the definition of "financial institution" or "creditor" would have to implement a red flags program only if it offers or maintains "covered accounts." A "covered account" includes (i) an account maintained by a financial institution or creditor for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and (ii) any other account offered or maintained by a financial institution or creditor with respect to which there is a reasonably foreseeable risk of identity theft. A CFTC covered account would include a margin account. SEC covered accounts would include brokerage accounts, mutual fund accounts and investment advisory accounts. According to the Release, there may be a foreseeable risk of identity theft for accounts that have been the target of identity theft, or accounts 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. Accounts with business entities are thought to pose a lower risk of identity theft.

Program Objectives, Elements and Administration

If a financial institution or creditor offers or maintains covered accounts, then it must implement a program designed to detect, prevent and mitigate identity theft. The program should be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its business.

A program should include policies and procedures to identify and detect red flags, respond to red flags once they have been detected and assess whether and how often to update the program.

A board of directors or committee of the board or, if an entity does not have a board, a designated senior management employee such as a chief compliance officer must approve the red flags program and be involved in its oversight, development and administration. Training is an additional and important aspect of the program; employees must be trained to implement the program effectively in order for an entity to meet its obligations under the new rules. Staff of the financial institution or creditor must provide to the board or designee, at least annually, a report addressing material matters related to the program and evaluate issues such as recommendations for material changes to the program. A financial institution or creditor may outsource its program or components of its program but must exercise appropriate and effective oversight of its service provider arrangements. Service providers should be required by contract to have policies and procedures to detect relevant red flags that may arise in the performance of their duties and either report them to the financial institution or creditor, or take appropriate steps to prevent or mitigate identity theft. Ultimately, however, the financial institution or creditor remains responsible for complying with the rules.

SEC and CFTC Guidelines

The SEC and CFTC issued guidelines for designing and implementing a program. A supplement to the guidelines identifies many specific types of red flags that should be considered in developing or updating a program.

The areas covered in the guidelines include (i) risk factors to consider (e.g., types of covered accounts, methods by which customers can access their accounts and the entity's previous experiences with identity theft); (ii) sources and categories of red flags to consider (e.g., alerts from consumer reporting agencies, suspicious documents, suspicious address changes, unusual activity related to a customer account and notices from customers regarding possible identity theft); (iii) policies and procedures that may be included in a program (e.g., identity verification and transaction monitoring procedures); (iv) appropriate responses to red flags that are detected (e.g., account monitoring, contacting the customer, changing security codes and notifying law enforcement); (v) factors to consider in updating a program (e.g., changes in account types and business arrangements and changes in methods of identity theft and detecting it); and (vi) methods for administering a program (e.g., board oversight and internal compliance reports).

Card Issuers

The new rules also set out the duties of financial institutions and creditors that issue debit and credit cards. The SEC and the CFTC acknowledged, however, that it is unlikely that entities subject to their respective authority issue debit or credit cards and that such entities, therefore, are unlikely to be subject to the card issuer rules.

Practical Considerations

Each SEC and CFTC regulated entity should determine whether it falls within the scope of the rules, meets the definition of either a financial institution or a creditor, and offers or maintains a covered account. If outside the rules after this initial assessment, each such entity should make periodic reassessments as to whether the rules apply.

* * * * * * * * * * * * * *

If you have any questions concerning the foregoing or would like additional information, please contact Daniel Schloendorn (212-728-8265, dschloendorn@willkie.com), Rita M. Molesworth (212-728-8727, rmolesworth@willkie.com), Martin R. Miller (212-728-8690, mmiller@willkie.com), Marc T. Foster (202-303-1151, mfoster@willkie.com), Marc J. Lederer (202-728-8624, mlederer@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Paris, London, Milan, Rome, Frankfurt and Brussels. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

May 2, 2013

Copyright © 2013 Willkie Farr & Gallagher LLP.