
April 11, 2013

SEC and CFTC Adopt Identity Theft Red Flag Rules Applicable to Certain Investment Advisers and Other Regulated Entities

Yesterday, the SEC and CFTC jointly adopted rules and guidelines requiring certain entities regulated by the agencies to adopt programs to detect red flags and prevent identity theft. The Dodd-Frank Act amended the Fair Credit Reporting Act (“FCRA”) to transfer responsibility for identify theft rules and the enforcement of the rules from the Federal Trade Commission to the SEC and the CFTC with respect to the entities they regulate. The SEC’s rules apply to an SEC-registered investment adviser, broker-dealer, or mutual fund that meets the definition of a “financial institution” or a “creditor” under the FCRA. The CFTC’s rules apply to entities such as commodity trading advisers, commodity pool operators, and futures commodity merchants.

During the SEC’s open meeting, Commissioner Luis Aguilar urged private fund advisers registered with the SEC to pay particular attention to the adopting release which offers a number of examples and illustrations that may assist these investment advisers in understanding whether they fall within the scope of the new rules. For example, the staff advised that certain investment advisers would meet the definition of a “financial institution” where they have the authority to pay bills or otherwise disburse funds to third parties from an investor’s account.

Entities that fall within the scope of the rules must adopt a program containing policies and procedures that are designed to detect and respond appropriately to identity theft red flags. The rules allow flexibility in determining which red flags may be relevant to the businesses and the accounts managed by different types of entities. Categories of red flags that regulated entities should consider including in their programs, as appropriate, include: alerts, notifications, or other warnings received from consumer reporting agencies or service providers; 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 others persons regarding possible identity theft.

The rules include guidelines to assist the relevant entities in the formulation and maintenance of programs that would satisfy the requirements of the rules. The program should include policies and procedures designed to:

- Identify relevant types of identity theft red flags.

-
- Detect the occurrence of those red flags.
 - Respond appropriately to the detected red flags.
 - Periodically update the identity theft program.

These entities must also provide staff training. The SEC's and CFTC's rules require that the identify theft red flag programs be overseen by an entity's board of directors or senior management.

Importantly, an entity that initially determines it does not need to have a program in place is required to periodically reassess whether it must develop and implement a one in light of changes in the accounts it offers or maintains.

The final rules will become effective 30 days after publication in the Federal Register, and the compliance date will be six months after the effective date. **As such, we anticipate the compliance date to be mid to late November 2013.** The SEC staff believes this seven-month period will give registered entities time to adopt policies and procedures, after which the staff will proceed with compliance examinations.

For a copy of the SEC's press release, see <http://www.sec.gov/news/press/2013/2013-57.htm>

For a copy of the final rules, see <http://www.sec.gov/rules/final/2013/34-69359.pdf>

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Yvonne Y. F. Chan

212-373-3255

ychan@paulweiss.com

Udi Grofman

212-373-3918

ugrofman@paulweiss.com

Robert M. Hirsh

212-373-3108

rhirsh@paulweiss.com

Michael S. Hong

212-373-3788

mhong@paulweiss.com

Marco V. Masotti

212-373-3034

mmasotti@paulweiss.com

Philip A. Heimowitz

212-373-3518

pheimowitz@paulweiss.com

Karen J. Hughes

212-373-3759

khughes@paulweiss.com

Amran Hussein

212-373-3580

ahussein@paulweiss.com

Stephanie R. McCavitt

212-373-3558

smccavitt@paulweiss.com

Jennifer A. Spiegel

212-373-3748

jspiegel@paulweiss.com