SHEARMAN & STERLING LLP

INVESTMENT FUNDS AND FINANCIAL INSTITUTIONS
ADVISORY & FINANCIAL REGULATORY

CLIENT PUBLICATION

May 10, 2013

SEC and CFTC Take Over Responsibility for "Red Flags" Identity Theft Rules and Provide Clarifications

If you wish to receive more information on the topics covered in this publication, you may contact your regular Shearman & Sterling contact person or any of the following:

Contacts

Nathan J. Greene
New York
+1.212.848.4668
ngreene@shearman.com

Jesse P. Kanach
Washington, DC
+1.202.508.8026
jesse.kanach@shearman.com

Lindi Beaudreault
New York
+1.212.848.8142
lindi.beaudreault@shearman.com

Azam H. Aziz
New York
+1.212.848.8154
aaziz@shearman.com

Lorna Xin Chen
Hong Kong
+852.2978.8001
lorna.chen@shearman.com

Robert Ellison
São Paulo
+55.11.3702.2220
robert.ellison@shearman.com

John W. Finley III
New York
+1.212.848.4346
sean.finley@shearman.com

Effective May 20, 2013, the US Securities and Exchange Commission and the US Commodity Futures Trading Commission will take on joint responsibility for administering and enforcing identity theft "red flags" rules that closely mirror other federal agencies' rules with which certain entities that the SEC and CFTC regulate have had to comply since at least December 31, 2010. The red flags rules now adopted by the SEC and CFTC (the "Rules"), like those of the other agencies, require certain financial institutions to adopt programs with detailed policies and procedures designed to detect, prevent, and mitigate identity theft, as we summarize below. Despite the lack of substantive change, the Rules are worth revisiting for some firms, as the SEC and CFTC have provided clarifications that their adopting release says "may lead some entities that had not previously complied with the [other federal agencies'] rules to determine that they fall within the scope of" the newly adopted Rules.[1]

I. Background

The emphasis under the Rules is on dealings with individuals, rather than with entities, and the Rules are part of an overlapping suite of US and state privacy-related regulations affecting the operations of funds, advisers and broker-dealers. A number of these privacy

[1] *Identity Theft Red Flags Rules*, SEC Release Nos. 34-69359, IA-3582, IC-30456 (April 10, 2013). The SEC refers to the Rules as "Regulation S-ID."

Contacts (cont.)

Laura S. Friedrich
New York
+1.212.848.7411
laura.friedrich@shearman.com

Etienne Gelencsér
Tokyo
+81.3.5251.0209
etienne.gelencser@shearman.com

Geoffrey B. Goldman
New York
+1.212.848.4867
geoffrey.goldman@shearman.com

Donna M. Parisi
New York
+1.212.848.7367
dparisi@shearman.com

Barnabas W.B. Reynolds
London
+44.20.7655.5528
barney.reynolds@shearman.com

Bradley K. Sabel
New York
+1.212.848.8410
bsabel@shearman.com

Russell D. Sacks
New York
+1.212.848.7585
rsacks@shearman.com

Paul S. Schreiber
New York
+1.212.848.8920
pschreiber@shearman.com

Bill Murdie
London
+44.20.7655.5149
bill.murdie@shearman.com

Charles S. Gittleman
New York
+1.212.848.7317
cgittleman@shearman.com

Richard Metsch
Hong Kong
+852.2978.8010
rmetsch@shearman.com

John Adams
London
+44.20.7655.5740
john.adams@shearman.com

regulations are summarized in a previous Shearman & Sterling client publication, *US Privacy Rules for Asset Management Businesses: Five Key Developments for 2010*.[2]

The SEC and the CFTC, in the cost-benefit analysis in their joint adopting release, conclude that upon the implementation of the Rules, regulated firms should see no real difference in the costs of compliance. However, the combined 230-plus pages dedicated to the Rules in the SEC's and CFTC's joint proposing and adopting releases – together with remarks like those of Norm Champ, Director of the SEC's Division of Investment Management, calling adoption of the Rules a key near-term priority of the SEC[3] – suggest that the SEC and CFTC may view their roles as more than mere custodians of rules formerly governed by other agencies. The Rules thus could become a more significant topic of examination by the SEC or CFTC (or by FINRA or the NFA). If so, firms may wish to take this rulemaking as an opportunity to reassess effectiveness of their current policies and procedures.

II. To Whom Do the Red Flags Rules Apply?

Each Regulated Entity (as defined below) must periodically consider whether it has substantive compliance obligations under the Rules – even if it concludes initially that it has engaged in no relevant activities that trigger such obligations. In particular, a Regulated Entity must determine initially, and then periodically, whether it is a "financial institution" or a "creditor," and if so, whether it offers or maintains any "covered accounts." (We define each of these terms below.) As part of that periodic determination, the financial institution or creditor must consider whether its accounts pose a risk of identity theft by considering: (1) the methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) previous experiences with identity theft.

SEC- and CFTC-Registered Entities

The Rules apply to most categories of SEC registrants and CFTC registrants (for purposes of this summary, "Regulated Entities"), including, for example:

- Any SEC-registered investment company
- Any investment company regulated by the SEC as a business development company

[2] That publication is available at: www.shearman.com/us-privacy-rules-for-asset-management-businesses--five-key-developments-for-2010-02-03-2010. Regulations discussed there include Regulation S-P, Regulation S-AM, the Massachusetts Data Security and Privacy Law, and the identity theft red flags rules of the US Federal Trade Commission ("FTC") that are the predecessors to the rules covered under this alert.

[3] See, e.g., Norm Champ, Director, Division of Investment Management, SEC, *Remarks to the IAA Investment Adviser Compliance Conference 2013* (March 8, 2013), available at http://www.sec.gov/news/speech/2013/spch030813nc.htm.

Contacts (cont.)

Pang Lee
Hong Kong
+852.2978.8005
pang.lee@shearman.com

David L. Portilla
New York
+1.212.848.4468
david.portilla@shearman.com

Michael P. Shin
New York
+1.212.848.8654
michael.shin@shearman.com

- Any investment company that operates as an employees' securities company under an SEC exemptive order
- Any SEC-registered investment adviser (but not "exempt reporting advisers")
- Any SEC-registered broker-dealer
- Any nationally recognized statistical rating organization (NRSRO), self-regulatory organization (SRO), municipal advisor, municipal securities dealer, and any other entity registered or required to register with the SEC under the US Securities Exchange Act of 1934, but not those that have simply registered securities under that Act or the US Securities Act of 1933 or which simply report information under the federal securities laws
- Any CFTC-registered 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")

The Rules apply not only to firms registered with the SEC or CFTC, but also to entities required to be registered with the SEC or CFTC. In addition, certain unregistered firms should consider, even if these Rules do not apply to them, whether another federal agency's red flags rules (such as those of the FTC) do apply. A non-US firm also may wish to consider whether the Rules may not apply to parts of its business.

The Rules impose substantive compliance obligations on those Regulated Entities that (i) are either "financial institutions" or "creditors" and (ii) handle "covered accounts."

Financial Institutions

For purposes of the Rules, a "financial institution" includes certain banks and credit unions, and any other person that directly or indirectly holds a "transaction account" belonging to an individual – that is, a deposit or an account on which the depositor or the account holder is allowed to make withdrawals by negotiable or transferable instrument, payment orders or withdrawals, telephone transfers, or other similar items for the purpose of making payments or transfers to third parties. The CFTC expressly lists as within the scope of "financial institution" any FCM, RFED, CTA, CPO, IB, SD, or MSP that directly or indirectly holds a transaction account belonging to a consumer.

Examples of financial institutions for SEC purposes include:

- A registered fund that offers check-writing privileges
- A registered fund that allows shareholders to provide instructions to wire redemption proceeds to a third party
- A registered adviser that regularly lends money to permit investors to invest in a fund managed by such registered adviser
- A registered adviser with the authority to direct an investor's redemption, distribution,

dividend, interest or other proceeds to third parties based on the investor's instructions

- A registered adviser authorized on behalf of an investor to withdraw assets from an investor's account to pay bills, or direct payments to third parties, regardless of whether the authority is based on the client's instructions or whether the investor's assets are held with a qualified custodian

However, a financial institution does not include a registered adviser authorized to withdraw money from an investor's account solely for the purpose of deducting its advisory fee.

Creditors

A "creditor" includes certain entities (again expressly including, for CFTC purposes, any FCM, RFED, CTA, CPO, IB, SD, or MSP) that regularly extend, renew, or continue credit; regularly arrange for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participate in the decision to extend, renew, or continue credit. The SEC definition is applicable to lenders that include:

- A registered broker-dealer offering margin accounts
- A registrant offering securities lending services or short selling services
- A registered adviser that regularly and in the ordinary course of business lends money to permit investors to make an investment in the fund, pending the receipt or clearance of an investor's check or wire transfer

The SEC noted, however, that a registered investment adviser is not a creditor solely because its private funds regularly borrow from third-party credit facilities pending receipt of investor contributions.

Covered Accounts

To be subject to substantive compliance obligations under the Rules, the financial institution or creditor must offer or maintain a "covered account." A "covered account" is (i) an "account" offered or maintained primarily for personal, family or household purposes that involves or is designated to permit multiple payments or transactions, and (ii) any other "account" offered or maintained with 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). An "account" is 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.

III. What Do the Rules Require a Regulated Entity to Do?

Each financial institution or creditor that offers or maintains one or more covered accounts must adopt an identity theft red flags program containing reasonable policies and procedures to:

1. Identify relevant red flags for the covered accounts that the Regulated Entity offers or maintains, and incorporate those red flags into the program;
2. Detect the occurrence of red flags;
3. Respond appropriately to the detected red flags; and
4. Periodically update the identity theft programs including any relevant red flags to reflect changes in risks to customers and to the safety and soundness of the Regulated Entity from identity theft.

Identifying Red Flags

The Rules adopt guidelines intended to assist Regulated Entities in the formulation and maintenance of programs that satisfy the Rules. A Regulated Entity must consider the following risk factors in identifying any red flags: (a) the types of covered accounts it offers or maintains; (b) the methods it provides to open and to access its covered accounts; and (c) its previous experiences with identity theft. A Regulated Entity will be afforded flexibility in determining which red flags are relevant to its business and the covered accounts it manages over time.

In addition, a Regulated Entity must consider including the following categories of red flags in its program:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- Presentation of suspicious documents, such as ID's that are apparently 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 the Regulated Entity's covered accounts.

Detecting Red Flags

An identity theft program's policies and procedures should address the detection of red flags. Such policies and procedures could include: (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. Regulated Entities already engaged in detecting red flags under other federal agencies' red flags rules may integrate existing policies and procedures developed for purposes of red flags compliance into their programs.

Responding to Red Flags

A Regulated Entity should develop an appropriate response to any detected red flags that is commensurate with the degree of risk presented. In determining an appropriate response to red flags, a Regulated Entity must consider aggravating factors that may heighten the risk of identity theft. Appropriate responses may include, for example, monitoring covered accounts for identity theft, or changing passwords or security codes that allow access to a covered account.

Periodically Updating an Identity Theft Program

Finally, a Regulated Entity should periodically update its program. Such an update may be based upon the following factors: (1) the experiences of the firm with identity theft; (2) changes in methods of identity theft; (3) changes in methods to detect, prevent, and mitigate identity theft; (4) changes in the types of accounts that the firm offers or maintains; and (5) changes in the business arrangements of the firm, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

IV. Administration of the Program

To emphasize the importance of the identity theft program, the Rules require that a program be approved at the level of the Regulated Entity's board of directors (or senior management). Moreover, the board (or senior management) must be

involved in the oversight, development, implementation, and administration of the program. Finally, Regulated Entities must exercise appropriate and effective oversight of service provider arrangements.

V. The Date of Effectiveness

The Rules are effective as of May 20, 2013, and Regulated Entities must comply by November 20, 2013. Again, however, many Regulated Entities will have been subject to other federal agencies' red flags rules since 2010 and so may conclude, on reviewing the current Rules, that no or few changes are required.

599 LEXINGTON AVENUE | NEW YORK | NY | 10022-6069