CLIENT UPDATE

SEC AND CFTC ISSUE FINAL RULES ON IDENTITY THEFT PROTECTION

WASHINGTON, DC
Satish M. Kini
smkini@debevoise.com

Kenneth J. Berman
kjberman@debevoise.com

Renee M. Cipro*
rmcipro@debevoise.com

NEW YORK
Byungkwon Lim
blim@debevoise.com

Lee A. Schneider
lschneider@debevoise.com

Aaron J. Levy
ajlevy@debevoise.com

On April 10, 2013, the Securities and Exchange Commission (the "SEC") and the Commodities Futures Trading Commission (the "CFTC") (together the "Commissions") jointly issued final rules on identity theft prevention (the "Final Rules") and accompanying guidance requiring certain regulated entities to adopt programs designed to detect "red flags" of identity theft and to respond appropriately to identity theft risks.[1] The Final Rules are substantially similar to the rules proposed by the Commissions in February 2012 (the "Proposed Rules").

The Final Rules potentially apply to SEC-registered investment advisers (including private fund advisers), broker-dealers and investment companies (including mutual funds, business development companies and employees' securities companies). The CFTC's Final Rules potentially apply to commodity trading advisers ("CTAs"), commodity pool operators ("CPOs"), futures commodity merchants ("FCMs"), swap dealers ("SDs"), major swap participants ("MSPs"), introducing brokers ("IBs") and retail foreign exchange dealers ("RFEDs").[2]

---

* Not yet admitted to the Bar of the District of Columbia. Admitted in Virginia only.

1 Identity Theft Red Flag Rules, 17 C.F.R. Part 248, Release No. 34-69359, IA-3582, IC-30456 (April 10, 2013), http://www.cftc.gov/PressRoom/PressReleases/pr6564-13

2 The Final Rules apply to all FCMs, CTAs, CPOs, SDs, MSPs, IBs, and RFEDs that are subject to the jurisdiction of the CFTC, regardless of whether such persons are required to register with the CFTC. *See* section 160.1 of the CFTC regulations. For example, a CPO that is exempt from registration under section 4.13(a)(3) of the CFTC regulations is nonetheless subject to the Final Rules.

During the SEC's open meeting, Commissioner Luis Aguilar urged private fund advisers newly registered with the SEC to pay close attention to the Final Rules.[3] As Commissioner Aguilar noted, many entities covered by the Final Rules already should have identity theft programs in place, pursuant to similar identity theft rules adopted in 2007 by other federal financial regulators.[4] This may not be the case for private fund advisers, however, and the SEC's adopting release offers a number of examples, discussed below, to help advisers understand whether they fall within the scope of the Final Rules.

An entity that falls within the scope of the Final Rules must adopt a program to detect and respond appropriately to identity theft red flags. The program should include policies and procedures designed to identify identity theft red flags, detect their occurrence and respond appropriately. The program must be overseen by an entity's board of directors, an appropriate committee thereof or a designated senior management employee and provide for staff training. An entity that initially determines it does not need to have a program in place (because it does not offer the types of accounts covered by the Final Rules) is required to periodically reassess whether changes in its accounts call on it to develop and implement a program.

The Final Rules will become effective 30 days after publication in the Federal Register. Affected entities will have six months thereafter to come into compliance with the new rules. Private fund advisers, CTAs, CPOs, FCMs, SDs, MSPs, IBs and RFEDs in particular should assess whether they are subject to the Final Rules and develop appropriate programs.

SCOPE OF THE IDENTITY THEFT RULES: WHICH FIRMS ARE REQUIRED TO HAVE AN IDENTITY THEFT PROGRAM?

Three key definitions determine whether an entity must adopt an identity theft program. To be covered by the Final Rules, the entity must be either a "*financial institution*" or a "*creditor*" and must offer and maintain one or more "covered accounts."

---

[3] Private fund advisers that continue to be exempt from registration with the SEC are not subject to the new rules.

[4] In 2007, the federal banking regulators and the Federal Trade Commission ("FTC") issued identity theft rules required by amendments to the Fair Credit Reporting Act ("FCRA"). The FTC's rules applied to firms regulated by the CFTC and SEC, because the CFTC and SEC were not included in the list of federal agencies required to adopt and enforce identity theft rules. This changed with the passage of the Dodd-Frank Wall Street Reform and Consumer Protect Act, which gave the Commissions rule-writing and enforcement authority under the FCRA provisions. See FCRA § 615(e)(1), 15. U.S.C. § 1681m(e)(1).

Financial Institution

A "financial institution" is defined to include certain banks and credit unions and "any other person that, directly or indirectly, holds a transaction account" belonging to an individual – that is, a natural person. A transaction account is an account that enables the accountholder to make payments or transfers to third parties.

In response to the Proposed Rules, certain commenters argued that investment advisers generally not "hold" transaction accounts and, thus, should be excluded from the definition of "financial institution." The SEC rejected this argument on the basis that advisers "who have the ability to direct transfers or payments from accounts belonging to individuals to third parties upon the individuals' instructions, or who act as agents on behalf of individuals" are susceptible to identity theft risks and should take steps to protect investors from such risks.

Under the SEC's approach, an investment adviser with authority (by power of attorney or otherwise) to withdraw money from an individual investor's account and direct payments to third parties according to the investor's instructions is a "financial institution," even if the investor's assets are physically held with a qualified custodian. The SEC also takes the position that a private fund adviser with authority, per an arrangement with a fund that it manages or with the individual investing in such fund, to direct an individual investor's investment proceeds (e.g., redemptions, distributions) to third parties is a "financial institution." By contrast, an adviser with authority to withdraw money from an investor's account only for the purpose of deducting the adviser's fees is not a financial institution and, thus, is not required to comply with the Final Rules. In addition, the SEC notes that an investment adviser that has a "narrowly-drafted" power of attorney with an investor under which the adviser has no authority to redirect the investor's investment proceeds to third parties or others upon instructions from the investor may not be a financial institution.

The SEC expects "most" advisers to private funds will be subject to the Final Rules based on an assumption that the private funds they manage will typically have at least one investor who is a natural person. Whether or not this assumption is correct for the "main funds" of many institutional managers, the Final Rules do not contain an exception for investors who are employees of the investment adviser. Additionally, some private fund advisers may engage in lending activities that would qualify them as creditors under the Final Rules, as explained next.

Creditor

A "creditor" is defined as a person who "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." Importantly, the term creditor is not limited to firms that extend credit to individuals; rather, firms that extend credit exclusively to entities may be creditors.

The SEC definition includes broker-dealers that offer margin accounts, securities lending services or short selling services. Some commenters had suggested that most investment advisers would not meet the "creditor" definition. In response, the SEC noted that an investment adviser could potentially be a creditor if it advances funds to an investor (other than for "expenses incidental to services provided by that adviser"). The SEC also noted that a creditor would include a private fund 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 explained that a private fund adviser would not be a creditor solely because the funds it manages regularly borrow from third-party credit facilities pending receipt of investor contributions.

The CFTC definitions of "financial institution" and "creditor" only apply to CTAs, CPOs, FCMs, SDs, MSPs, IBs, and RFEDs that meet the above definitions. Importantly, the Final Rules apply to all FCMs, CTAs, CPOs, SDs, MSPs, IBs and RFEDs that are subject to the jurisdiction of the CFTC, regardless of whether such persons are required to register with the CFTC. For example, a CPO that is exempt from registration under 4.13(a)(3) of the CFTC regulations is nonetheless subject to the Final Rules.

Covered Accounts

As noted, a financial institution or creditor must establish a red flags program only if it offers or maintains a "covered account." A covered account includes both (a) an account offered or maintained "primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions;" and (b) "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" (emphasis added).[5]

[5] The first prong of the SEC's definition includes brokerage accounts with a broker-dealer and accounts maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; the first prong of the CFTC's definition includes margin accounts. An "account" is defined as a "continuing relationship established by a person

The first prong of this definition applies exclusively to accounts that a firm holds for individuals, but the second prong may include accounts offered not only to individuals but also to businesses and other entities. The second prong also requires a subjective judgment: Under the second prong, financial institutions and creditors will need to determine whether the business and personal accounts they offer pose a risk of identity theft. In this regard, the Commissions acknowledge in the adopting release that some financial institutions and creditors engage predominantly in transactions with businesses, where the risk of identity theft is minimal. In these situations, a firm may determine that the accounts it offers do not pose "a reasonably foreseeable risk" of identity theft and, therefore, the firm may decide that it does not maintain covered accounts and need not develop an identity theft program. Such a determination would need to be reassessed periodically.

To determine if its accounts pose a risk of identity theft, a firm must review (a) the methods it uses to open account (e.g., does the firm permit accounts to be opened on the internet or otherwise remotely rather than face-to-face); (b) the methods it uses to provide access to access to accounts; and (c) its previous experiences with identity theft (e.g., has the firm or its accounts been victims of identity theft). The Commissions indicate that these periodic risk determinations will need to be documented.

IMPLEMENTATION AND ADMINISTRATION OF THE IDENTITY THEFT RED FLAGS PROGRAM: WHAT MUST FIRMS DO?

A financial institution or creditor that offers or maintains covered accounts must develop and implement a written identity theft program appropriate for the size and complexity of the firm. The program must contain four elements and include appropriate oversight.

Elements of a Program

The final rules and a set of accompanying guidelines, which are intended to assist firms with compliance, set out four elements required in an identity theft program.

- *Identifying red flags*. The program must include reasonable policies and procedures to identify "red flags" of identity theft and incorporate those red flags into the program. These red flags must be tailored so that they are relevant for the covered accounts that a firm offers. The guidelines accompanying the Final Rules include categories of red flags a firm should consider: (a) alerts, notifications or other warnings received from

with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes."

consumer reporting agencies or service providers; (b) presentation of suspicious documents, such as documents that appear to have been altered or forged; (c) presentation of suspicious personal identifying information, such as suspicious address change; (d) unusual use of, or other suspicious activity related to, a covered account; and (e) notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts.

- *Detecting red flags*. Policies and procedures should be developed to detect red flags. Procedures could include, for example, (a) obtaining identifying information about, and verifying the identity of, a person opening a covered account and (b) authenticating customers, monitoring transactions and verifying validity of change of address requests. Firms may incorporate the steps they take to comply with anti-money laundering and customer identification program requirements into this element of their identity theft programs.
- *Responding to red flags that are detected*. Firms must develop risk-based responses when identity theft risks are detected. Such responses may range from monitoring covered accounts; contacting the customer; changing any passwords, security codes or other security devices that permit access to covered accounts; or notifying law enforcement.
- *Periodically updating the program*. Finally, firms must have reasonable policies and procedures to update periodically their identity theft programs (including the relevant red flags). The Final Rules do not specify how frequently updating should occur but, instead, indicate that updating should be based on factors such as: experiences with identity theft, changes in methods of identity theft, changes in identity theft detection methodology, changes in accounts offered and changes in business arrangements (including corporate transactions and service provider relationships).

Oversight and Administration

The Final Rules require the board of directors, an appropriate board committee or a designated senior management employee[6] of a financial institution or creditor to be involved in the oversight, development, implementation and administration of the identity theft program.

Specifically, the board, appropriate committee or senior management employee should: (a) assign specific responsibility for the program's implementation; (b) review reports

[6] In the adopting release, the SEC notes that the designated senior management employee who is responsible for the oversight of a broker-dealer's, investment company's or investment adviser's program may be the entity's chief compliance officer.

prepared by staff regarding compliance with the Final Rules; and (c) approve material changes to the program as necessary to address changing identity theft risks.

Staff of the entity responsible for the program should report to the board, board committee or senior management employee "at least annually" on its program. The report should address the effectiveness of the program, any significant identity theft incidents and management's response and any recommended material changes to the program.

Additionally, the guidelines make clear that when a firm engages a service provider to perform an activity in connection with one or more covered accounts, the firm must ensure that the service provider is performing such services in accordance with "reasonable policies and procedures" designed to detect, prevent and mitigate the risk of identity theft. This means that firms should ensure that service providers are contractually obligated to have appropriate policies and procedures in place and should oversee and monitor their service providers' conduct under those policies and procedures.

Finally, the Final Rules require financial institutions and creditors to train their staff as necessary to implement the program.

CONCLUSION

Firms that fall within the definition of "financial institution" or "creditor" under the Final Rules and have not yet adopted identity theft programs will need to assess their customers and account offerings to determine what activities could bring their firm within such definitions. Firms that are subject to the Final Rules will need to develop policies and procedures to identify, detect and respond to red flags of identity theft. They may also have to supplement the resources devoted to compliance to assure that they are sufficient to address this new responsibility.

* * *

Please do not hesitate to contact us with any questions.

April 16, 2013