Client Alert

April 19, 2013

SEC and CFTC Issue Identity Theft Rules

By Daniel A. Nathan and Ana-Maria Ignat

Today, April 19, 2013, the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") published in the Federal Register rules and guidelines requiring their respective regulated financial institutions to establish programs to address the risks of identity theft, that is, "fraud committed or attempted using the identifying information of another person without authority." The SEC's rules apply to broker-dealers, mutual funds, investment advisers, and other financial institutions and creditors; the CFTC's rules apply to futures commission merchants, retail foreign exchange dealers, commodity trading advisers, commodity pool operators, swap dealers, and major swap participants. The final rules will become effective on May 20, 2013, and compliance is required by November 20, 2013.

The new rules draw more firms into the ambit of the requirement to have identity theft procedures. As SEC Commissioner Luis A. Aguilar noted, investment advisers registered under the Investment Adviser Act, particularly the private fund and hedge fund advisers that are recent registrants with the SEC, might not have existing identity theft red-flag programs, and will need to pay particular attention to the rules being adopted.

The SEC and CFTC were not among the agencies Congress required in the 2003 amendments to the Fair Credit Reporting Act ("FCRA") to issue rules and guidelines on detecting, preventing, and mitigating identity theft. But, in 2007, the federal banking agencies and the Federal Trade Commission ("FTC") issued final identity theft red-flag rules that applied to entities under their respective jurisdictions, and FINRA issued guidance applying the requirements of the FTC's rule to certain entities registered with the CFTC and the SEC, such as futures commission merchants, broker-dealers, investment companies, and investment advisers.

The Dodd-Frank Wall Street Reform and Consumer Protection Act amended the FCRA to add rulemaking responsibility and enforcement authority to the CFTC and SEC with respect to all the entities subject to each agency's enforcement authority. In February 2012, the two Commissions proposed rules requiring the entities they regulate to establish red-flag, that is, written identity theft prevention, programs. The final rules are substantially similar to the rules the other agencies adopted in 2007.

WHO IS COVERED?

The final rules require "financial institutions" and "creditors" that offer and maintain "covered accounts" to develop and implement a written identity theft prevention program, including reasonable policies and procedures designed to identify, detect, prevent, and mitigate identity theft. The rules contain guidelines to assist in the design and maintenance of programs that would satisfy the requirements of the rules. Instead of defining red flags or requiring specific policies and procedures to identify red flags, the Commissions provide financial institutions and creditors with "flexibility in determining which red flags are relevant to their businesses and the covered accounts they manage over time," allowing them "to respond and adapt to new forms of identity theft and the attendant risks as they arise."

To identify covered accounts, the SEC provides the examples of an account with a broker-dealer or an account maintained by a mutual fund or an agent permitting wire transfers or other payments to third parties. The Commissions notes that the definition of a "covered account" is "deliberately designed to be flexible to allow the financial institution or creditor to determine which accounts pose a reasonably foreseeable risk of identity theft."

The final rules apply to "financial institutions" and "creditors" subject to the Commissions' enforcement authority, and do not exclude any entities registered with the two agencies from their scope. The term "financial institution" is defined as a bank or another entity that maintains "transaction accounts" for consumers. The term "creditor" has the same meaning as in the Equal Credit Opportunity Act ("ECOA") – that is, a person that permits deferral of payment of a debt – but is limited to creditors that obtain consumer reports, furnish information to consumer reporting agencies, or advances funds to a person.

In its Federal Register release, the SEC provides illustrations of SEC-regulated entities that could fall within the meaning of the term "financial institution" for the purposes of these rules because they hold transaction accounts belonging to individuals: (i) a broker-dealer offering custodial accounts; (ii) a registered investment company allowing investors to make wire transfers to other parties or offering check-writing privileges; and (iii) an investment adviser that directly or indirectly holds transaction accounts and is permitted to direct payments or transfers to third parties.

As for the definition of "creditor": the CFTC's rules define it to include "any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant 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." In contrast, the SEC's definition of "creditor" refers to the definition of creditor under the FCRA, that is, a creditor as defined in the ECOA, and omitted references to specific types of lending, such as margin accounts, securities lending services, and short-selling services, initially included in the proposed rules, to avoid an inadvertently broad meaning.

Under the Rules, financial institutions and creditors periodically have to determine whether they offer or maintain covered accounts by conducting a risk assessment considering the methods provided to open and access accounts, and their previous experiences with identity theft.

WHAT ARE REASONABLE POLICIES AND PROCEDURES?

Identification of relevant red flags

In identifying relevant red flags, financial institutions or creditors should incorporate red flags from sources such as actual incidents of identity theft experienced, methods of identity theft identified, and applicable supervisory guidance, and consider risk factors such as the types of accounts offered or maintained, the methods to open and access accounts, and previous experiences with identity theft.

The program should include, as appropriate, the following red flags: (a) alerts or notifications from consumer reporting agencies; (b) the presentation of suspicious documents or suspicious personal identifying information; (c) suspicious or unusual activity related to a covered account; and (d) notice from customers, victims of identity theft, or law enforcement authorities regarding potential identity theft related to covered accounts.

Detection of red flags

Reasonable policies and procedures will address the detection of red flags by: (a) obtaining identifying information and verifying the identity of a person opening a covered account; and (b) authenticating customers, monitoring transactions, and verifying the validity of address changes in the case of existing covered accounts.

Appropriate response to red flags detected: prevention and mitigation of identity theft

The program's policies and procedures must provide for appropriate responses to detected red flags that are commensurate to the risks posed, taking into consideration factors that might heighten the identity theft risks. Heightened risks might result, for example, from data security incidents resulting in unauthorized access to a customer's account records, or from the customer providing information related to the covered account to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate prevention and mitigation steps may include: (a) monitoring the covered account for evidence of identity theft; (b) contacting the customer; (c) changing passwords, security codes, and other security devices permitting access to a covered account; (d) reopening a covered account with a new account number; (e) closing an existing covered account; (f) not attempting to collect on a covered account or not selling it to a debt collector; or (g) notifying law enforcement.

Administration of the red-flag program

Finally, the rules require financial institutions and creditors to have reasonable policies and procedures to periodically update their programs to reflect changing risks to customers and the soundness of the financial institution or creditor from identity theft. The guidelines list certain factors on which financial institutions and creditors could base their periodic updates, including: their experience with identity theft; changes in methods of identity theft; changes in methods to detect, prevent, or mitigate identity theft; changes in the types of accounts offered or maintained; and changes in the business arrangements, including mergers, acquisitions, joint ventures, and service provider arrangements.

The rules also require that the initial written program be approved by, for example, the board of directors, and be subject to at least annual reporting on compliance with the rules to the board of directors. Financial institutions and creditors are required to train their staffs to effectively implement the program.

Oversight of Service Providers

Significantly, the final rules also require financial institutions and creditors to takes steps to ensure that the activity of any service providers is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. While the rules do not provide for specific oversight measures, the accompanying guidelines provide that a financial institution or creditor could contractually require service providers to have policies or procedures to detect relevant red flags that may arise in the performance of the service provider's activities, and report the red flags to the financial institution or creditor or take appropriate measures to prevent or mitigate identity theft. In the commentary, the Commissions noted that they expect the contractual arrangement to include a requirement that documentation be provided by the service provider to the financial institution or creditor to enable it to assess compliance with the identity theft red flag rules, and that

financial institutions and creditors remain legally responsible for compliance with the rules regardless of their outsourcing of any aspect of the red flags program operation.

Contact:

Jay G. Baris
(212) 468-8053
jbaris@mofo.com

Hillel T. Cohn
(213) 892-5251
hcohn@mofo.com

Randall J. Fons
(303) 592-2257
rfons@mofo.com

Kelley A. Howes
(303) 592-2237
khowes@mofo.com

Ana-Marie Ignat
(202) 887-1561
aignat@mofo.com

Daniel A. Nathan
(202) 887-1687
dnathan@mofo.com

Anna T. Pinedo
(212) 468-8179
apinedo@mofo.com

Andrew M. Smith
(202) 887-1558
andrewsmith@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.