The 'Red Flags' Rule: Are You Ready?


Because the Rule has been adopted by the Federal Trade Commission (“FTC”) as opposed to the U.S. Securities and Exchange Commission or the Financial Industry Regulatory Authority (“FINRA”) and because its application has been postponed, it does not appear to have created a lot of news in the financial press. Nevertheless, the requirement is looming and it applies to more firms than one initially might think.

Essentially, the “Red Flags” Rule requires firms to develop and implement an approved written Identity Theft Prevention Program for fighting identity theft among new and existing accounts.[2]

Identity theft is a fraud committed using the identifying information of another person.[3] For broker-dealers, it is helpful to think of identity theft in the context of protection of customer information.[4]

Five months ago, FINRA alerted firms to this requirement and advised that even though it is not a FINRA rule, failure to comply with the FACT Act will be considered a violation of FINRA Rule 2110.[5] In addition, FINRA has just listed the Rule on its list of examination priorities for 2009.[6]

The hardest part of the Rule may be determining whether a firm is subject to it. If a firm must comply, it should be able to adapt its other policies and procedures to draft an adequate program.

In order to assess whether the Rule is applicable, firms first must determine whether they meet the definition of a “financial institution” or a “creditor.” If they are either a financial institution or creditor, they then must determine if they hold “covered accounts.”
The term financial institution means a depository institution that holds an individual “transaction account”[7] which allows for withdrawals, payments, or transfers to third parties through telephone transfers, checks, debit cards or other similar instruments.[8]

Therefore, firms that provide their individual customers with check-writing or debit/credit card privileges meet the definition of a financial institution.[9]

A “creditor” by definition of the Rule is a person/entity that regularly extends or arranges for the extension, renewal or continuation of credit.[10]

Thus, a firm that provides margin, arranges for margin or participates in the decision to arrange or extend margin to its customers will meet the definition of a creditor.

Consequently, even firms that have solely institutional clients can be subject to the Rule if they extend credit or arrange for credit for any of their customers.[11]

Once a firm has determined that it is a “financial institution” or “creditor,” it then must determine if it maintains any “covered accounts.”

A covered account is an account that is either a retail account, offered or maintained primarily for personal use and designed to permit multiple payments or transactions, or it is any other account for which there is a foreseeable risk to customers from identity theft.[12]

Apparently, introducing broker-dealers should assume that even though the extension of credit for margin and check-writing privileges may actually be services offered by the clearing firm, the introducing broker is required to comply with the Rule as it is the entity that has the direct relationship with the customer.

Of course, if necessary or even if helpful, the introducing broker can and should seek assistance from its clearing firm by requesting reports and other data from the clearing firm.

For those firms that conduct an assessment and determine that they are not bound by the Rule, the Rule requires a periodic reassessment of the firm’s activities and accounts to determine if it later becomes subject to the Rule.[13]

If a firm meets the definitions of a financial institution or creditor maintaining covered accounts then it must develop and implement a program.

According to the FTC, the program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:

1) Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program;
2) Detect red flags that have been incorporated into the Program;

3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

4) Ensure the program is updated periodically to reflect changes in risks from identity theft.[14]

Once the program has been created, it must be approved by the firm’s board of directors or a designated person in senior level management, such as the chief compliance officer, chief legal officer or president (if there is no board of directors).

The board or the designated senior level officer is then responsible for the oversight and implementation of the program, on a going-forward basis, which includes the training of staff, as necessary to ensure its effective implementation.

Also, if any part of the program is outsourced to a third-party service provider, it is the responsibility of the board or the senior manager to ensure that there is effective oversight of that service provider.[15] At a minimum, such review should include ensuring that the third-party service provider has its own program.

Firms that are subject to the Rule and which are required to create a program will be able to use their AML and Regulation S-P policies and procedures as a framework from which to create a Program.

While reinventing the wheel is not required, a specific written Program should be drafted for the Rule rather than slapping a “Red Flags Rule” cover page on existing AML and Regulation S-P procedures.

It is recommended that firms use the guidance provided in Appendix A of the Rule. The appendix specifically suggests that the Program have five parts:

1) Identifying Relevant Red Flags;

2) Detecting Red Flags;

3) Preventing and Mitigating Identity Theft;

4) Updating the Program; and

5) Methods for Administering the Program.

Furthermore, the FTC provided as a supplement to Appendix A, 26 illustrative examples of red flags in connection with covered accounts. These 26 examples are divided up into five categories and should be considered when creating a program:[16]
1) Alerts, notifications, or other warnings received from consumer reporting agencies;

2) The presentation of suspicious documents;

3) The presentation of suspicious personal identifying information;

4) The unusual use of, or other suspicious activity related to, a covered account; and

5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.

Given that FINRA highlighted this Rule under New Developments in its 2009 Examination Priorities letter, firms should expect that examiners will be asking to review the Program of applicable firms beginning May 1, 2009.

As it is a new requirement, FINRA likely will be focused on ensuring that applicable firms have created an adequate written program and that they followed all of the required steps for approval.

Those firms that have followed the guidance provided by the FTC and divided the program into the suggested five parts and address how they will detect the 26 examples cited in the supplement will make it easy for the examiner to note that the program has all of the required parts.

It is suggested that in reviewing the 26 examples, firms simply note what protocol they have in place to cover such a situation or where a situation is inapplicable, that the written program so states.

In this article, we have covered only the “Red Flags” portion of the FACT Act. Firms should be aware that there are other parts of the FACT Act that deal with the issuance of debit/credit cards and the use of consumer reports from a consumer reporting agency.[17]

May 1, 2009 is fast approaching, so make sure that an analysis has been conducted and if applicable a program has been created and implemented. So that you can say: “I am ready!”

--By Cheryl L. Haas-Goldstein and Gregory S. Amoroso, Sutherland Asbill & Brennan LLP

Cheryl Haas-Goldstein is a partner with Sutherland in the firm's Atlanta office. Gregory Amoroso is a securities consultant for Sutherland.

The opinions expressed are those of the authors and do not necessarily reflect the views of Portfolio Media, publisher of Law360.


[17] For more information about these rules or the “Red Flag” Rule go to www.ftc.gov.