Regulatory Notice 08-69

Fair and Accurate Credit Transactions Act of 2003

Alert to Member Firms About the Federal Trade Commission's FACT Act Regulations and the Announcement of the FTC's Decision to Delay Enforcement of the Red Flags Rule until May 1, 2009

November 2008

Notice Type

- Guidance
- Special Alert

Suggested Routing

- Compliance
- Internal Audit
- Legal
- Operations
- Senior Management
- Systems
- Training

Key Topics

- Changes of Address
- Consumer Reports
- Covered Accounts
- Creditors
- FACT Act
- Financial Institutions
- Identity Theft
- Notice of Address Discrepancy
- Privacy
- Red Flags
- Transaction Accounts

Executive Summary

FINRA is issuing this *Notice* to alert member firms about the Federal Trade Commission's (FTC's) Fair and Accurate Credit Transactions Act of 2003 (FACT Act) regulations and the FTC's decision to delay enforcement of the Red Flags Rule until **May 1, 2009**, to give member firms additional time to develop and implement their procedures. By that date, member firms subject to these regulations must have in place a written program to identify, detect and respond to patterns, practices or specific activities that could indicate identity theft.

The mandatory compliance date for the other FTC regulations approved at the same time as the Red Flags Rule remains **November 1, 2008**. Those regulations require any member firms that issue credit or debit cards to have reasonable policies and procedures to assess the validity of change-of-address notifications. Also, member firms that use consumer reports must develop reasonable policies and procedures to respond to the receipt of a consumer reporting agency's notice of address discrepancy. This *Notice* describes these FTC rules. Member firms are reminded that these are not FINRA Rules, and except as noted below, questions concerning these rules should be directed to the FTC.

To view the *Federal Register* notice of the FACT Act Regulations go to *www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf*.

FINRA
Financial Industry Regulatory Authority

Background & Discussion

The Federal Trade Commission (FTC) and the federal banking regulators have issued joint regulations[1] implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[2] As discussed in greater detail below, the FTC's regulations, which apply to most member firms, require that:

- Each financial institution or creditor develop and implement a written program to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or the maintenance of certain existing accounts (referred to as the Red Flags Rule);
- Each credit and debit card issuer assess the validity of change-of-address notifications; and
- Each user of consumer reports develop reasonable policies and procedures to respond to the receipt of a consumer reporting agency's notice of a consumer address discrepancy.

Member firms should understand that the purpose of this Notice is informational only. Its purpose is solely to inform member firms about federal regulations, which FINRA has neither engaged in rulemaking nor has the authority to interpret. Nevertheless, given the importance and possible application of these regulations to member firms, FINRA believes it is important to provide this Notice in addition to what has been published in the Federal Register. Member firms should not rely on this Notice as a substitute for their understanding and application of these regulations and should seek their own counsel to address any issues under these regulations. As noted at the conclusion of this Notice, the FTC has indicated its willingness to work with FINRA in addressing industry-wide questions pertaining to the application of these provisions to member firms.

A. Red Flags Rule

The FTC's Red Flags Rule requires a member firm that is a "financial institution" or "creditor" offering or maintaining "covered accounts" to develop, implement and administer a Written Identity Theft Prevention Program (Program) to detect, prevent and mitigate identity theft in connection with the opening of a covered account or the maintenance of any existing covered account. The Red Flags Rule also requires every member firm that is a financial institution or creditor (even those that have initially determined that they do not need to have a Program) to periodically reassess whether it offers or maintains covered accounts that would require it to have in place a written Program.

1. Determining the Applicability of the Red Flags Rule to Member Firms

There are several key definitions to determine whether the Red Flags Rule applies to a member firm. Specifically, the Red Flags Rule applies to a "financial institution" or "creditor." As a threshold matter, the member firm must first determine whether it is a financial institution or creditor. The term "financial institution" means a depository institution or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.[3] The term "transaction account" means an account that permits the account holder to make withdrawals for payment or transfer to third parties of funds via telephone transfers, check, debit card or other similar items.[4] The term "consumer" as used in the definition of financial institution reaches only individuals.[5] As a result, a member firm without any individuals as clients would not be deemed to be a financial institution.

The term "creditor" means any person who regularly extends, renews, or continues credit or regularly arranges for the extension, renewal or continuation of credit.[6] Therefore, if a member firm, acting as either an introducing or clearing firm, provides a customer with margin – a form of credit – it will be deemed to be a creditor for purposes of the Red Flags Rule. A member firm also will be deemed to be a creditor if it extends credit, or arranges to extend credit, to any of its customers in any other context, such as, arranging loans. A member firm that is not considered a financial institution because it has only institutional customers could still be a creditor if it extends credit, or arranges to extend credit, for any of its customers.

Once a member firm determines that it is either a financial institution or creditor, it must then analyze whether it has "covered accounts." The term "covered accounts" is defined as (1) an account offered or maintained primarily for personal, family or household purposes that is designed to permit multiple payments or transactions; or (2) any other account for which there is a reasonably foreseeable risk to customers or safety and soundness of the member firm from identity theft, including financial, operational, compliance, reputation or litigation risks.[7]

Each member firm that is a financial institution or creditor should carefully analyze its customers and accounts to determine the extent to which it must comply with the FTC's Red Flags Rule.[8] While the definition of "covered accounts" in clause (1) generally applies only to retail accounts, the alternative definition in clause (2) would include any type of account (including institutional accounts) if the member firm determines that those accounts pose a reasonably foreseeable risk to its customers or to its own safety or soundness from identity theft.

Member firms should also be aware that a firm that determines it is not a financial institution or creditor for purposes of the FTC's regulations should consider having procedures in place to reassess that determination if there is a change in business operations, such as a change of business model or the offering of a new business line or product.

2. Development and Implementation of the Program; Consideration of Guidelines

A member firm subject to the Red Flags Rule as discussed above, must develop and implement a Written Identity Theft Program that is appropriate to that firm's size and complexity and the nature and scope of its business. At a minimum, the Program must include reasonable policies and procedures to:

- Identify relevant red flags for the covered accounts that the member firm offers or maintains and incorporate those red flags into its Program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the member firm from identity theft.[9]

A member firm that is required to implement a Program must also consider the Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation (Guidelines) and include in its Program those guidelines that are appropriate.[10] These guidelines are intended to assist financial institutions and creditors in formulating and maintaining a Program. In addition, member firms should review, and implement where appropriate, the supplement to the Guidelines, which contains 26 illustrative examples of red flags.[11] Member firms already may be engaged in detecting some red flags through their requisite anti-fraud and anti-money laundering procedures. Accordingly, a member firm may consider whether such procedures can be adapted, to the extent appropriate, into its Program.[12]

3. Administration of the Program

A member firm that is required to develop and implement a Program must provide for its continued administration[13] and must:

- Obtain approval of the initial written Program from either its board of directors, an appropriate committee thereof, or (if there is no board of directors) a designated employee at the level of senior management;
- Involve the board of directors, an appropriate committee thereof or a designated employee at the level of senior management in the oversight, development implementation and administration of the Program;
- Train staff, as necessary, to effectively implement the Program; and
- Exercise appropriate and effective oversight of service provider arrangements.[14]

Member firms should also be aware of their obligations with respect to third-party service providers. Specifically, whenever a member firm engages a service provider to perform an activity to which the requirements of the Program would apply if the firm itself was performing the activity, the member firm must ensure that the service provider's activity is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.[15] For example, a member firm could contractually require the service provider to have policies and procedures to detect relevant red flags that may arise in the performance of its activities and either report the red flags to the member firm or to take appropriate steps to prevent or mitigate identity theft.[16]

4. Periodic Identification of Covered Accounts

Member firms that are financial institutions or creditors under the Red Flags Rule must periodically determine whether they offer or maintain covered accounts.[17] Further, as a part of this determination, the member firm must conduct a risk assessment to determine whether it offers or maintains covered accounts for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the member firm from identity theft, taking into consideration:

- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.[18]

B. Special Rules for Card Issuers

The FTC also issued rules that require any member firm considered to be a financial institution or creditor, as defined above, that issues credit or debit cards to have reasonable policies and procedures to assess the validity of any address change notifications the member firm receives.[19] Specifically, a member firm that receives an address change notification and, within at least 30 days, a request for an additional or replacement card, may not issue an additional or replacement card until it has either:

- Notified the cardholder of the request at the cardholder's former address or via any other means of communication that the member firm and the cardholder have previously agreed to use, and provided the cardholder with a reasonable means of promptly reporting incorrect address changes; or
- Otherwise assessed the validity of the change of address in accordance with the policies and procedures established in its Program.[20]

A member firm's notice to the cardholder, regardless of whether it is in either written or electronic form, must be clear and conspicuous and be provided separately from the member firm's regular correspondence with the cardholder.[21]

A member firm may also comply with these validation requirements if it validates an address using the methods described above before it receives a request for an additional or replacement card.[22]

C. Special Rules for Users of Consumer Reports

The FTC also has issued rules requiring any member firm requesting a consumer report on an individual from a consumer reporting agency (CRA) to develop reasonable policies and procedures to use if it receives a notice of address discrepancy[23] from the CRA. The policies and procedures should be designed to enable the member firm to form a reasonable belief that it has the correct consumer report.[24] This obligation exists regardless of whether the member firm receives the notice of address discrepancy for a consumer report requested in connection with the opening of an account or in other circumstances in which the member firm already has a relationship with the consumer, such as when the customer applies for margin privileges for an existing account.[25] Therefore, if a member firm requests a consumer report about a new or existing customer and receives a notice of address discrepancy, the member firm must be able to form a reasonable belief that the consumer report actually relates to the customer in question.

The FTC's rules provide examples of reasonable policies and procedures member firms can use to form a reasonable belief about the identity of the customer. One method would be to verify the information in the consumer report directly with the customer.[26] Alternatively, a member firm could compare the information in the consumer report with:

- Information obtained and used to verify the individual's identity in accordance with the requirements of the member firm's Customer Information Program (CIP);[27]
- Information maintained in its own records, such as applications, change-of-address notifications, other customer account records or retained CIP documentation; or
- Information obtained from third-party sources.[28]

Generally, a member firm should use its CIP information to form a reasonable belief about an individual's identity only in connection with an account opening. However, if the member firm has received a notice of address discrepancy regarding a consumer report about an existing customer and the member firm has already met its CIP obligations, the member firm should use the other examples listed above (*e.g.*, verifying the information directly with the customer, information obtained from third-party sources, etc.) to form its reasonable belief that the consumer report is about the correct individual.[29]

If a member firm cannot establish a reasonable belief that it has received the correct consumer report, the member firm should not use that report.[30] A member firm should be aware that other laws may also apply to a situation where it has received an incorrect consumer report. For example, in the case of account openings, if the member firm cannot establish a reasonable belief that it knows the true identity of the customer, it will need to follow its CIP obligations, which may involve not opening the account.[31] Additionally, a notice of address discrepancy may be a red flag and require an appropriate response under the member firm's Written Identity Theft Prevention Program.[32]

Finally, a member firm must furnish a consumer's address that it has reasonably confirmed is accurate to the CRA from which it received a notice of address discrepancy when the member firm:

- Can form a reasonable belief that the consumer report relates to the individual about whom the member firm requested the report;
- Establishes a continuing relationship with the customer; and
- Regularly and in the ordinary course of business furnishes information to the CRA.[33]

A member firm may reasonably confirm an address is correct by:

- Verifying the address with the customer;
- Reviewing its own records to verify the address of the customer;
- Verifying the address through a third-party; or
- Using other reasonable means.[34]

Future Interpretive Guidance

As previously noted, this *Notice* describes rules of the Federal Trade Commission, and the FTC is responsible for interpreting and applying these rules. Nevertheless, the FTC has indicated a willingness to work with FINRA to resolve on a consistent and industry-wide basis, interpretive questions that arise under these rules as applied to broker-dealers. Accordingly, FINRA invites member firms to contact FINRA's Office of General Counsel at (202)728-8071 with any questions regarding the regulations that pose significant interpretive challenges. Questions about compliance with the FACT Act Rules generally should be directed to the FTC.

Mandatory Compliance Date

Full compliance with the FTC's regulations was originally required by November 1, 2008. However, during the course of the FTC's education and outreach efforts following publication of the regulations, the FTC learned that some industries and entities within the FTC's jurisdiction were confused and uncertain about their coverage under the rule, especially the Red Flags Rule. Many entities also noted that because they generally are not required to comply with FTC rules in other contexts, they had not followed or even been aware of the rulemaking, and therefore learned of the requirements of the rule too late to be able to comply by November 1, 2008. Given this confusion and uncertainty, the FTC has delayed the enforcement of the Red Flags Rule until **May 1, 2009**, to allow these entities to develop and implement their programs.

Endnotes

1 *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 FR 63718 (November 9, 2007) (Joint Final Rules and Guidelines of the FTC, Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA)).

2 *See* Pub. L. 108-159 (amending Section 615 of the Fair Credit Reporting Act of 1970 (FCRA) and adding new Section 605(h)(2)).

3 The term "financial institution" is specifically defined as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account . . . belonging to a consumer." 16 CFR 681.2(b)(7); 15 U.S.C. 1681a(t).

4 A "transaction account" is specifically defined as "a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts." 12 U.S.C. 461(b)(1)(C).

5 15 U.S.C. 1681a(c).

6 The term "creditor" specifically means "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit." *See* 16 CFR 681.2(b)(5); 15 U.S.C. 1681a(r)(5); and 15 U.S.C. 1691a(e).

7 The term "covered account" specifically means:

> (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
>
> (ii)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, including financial, operational, compliance, reputational, or litigation risk.
>
> 16 CFR 681.2(b)(3).

8 Member firms, are reminded that the just and equitable principles of trade underpinning NASD Rule 2110 prohibit conduct that, to any degree, is illegal under any applicable law. Accordingly, a member firm subject to the FTC's Red Flags Rule that does not comply with the Red Flags Rule will be considered to have violated NASD Rule 2110.

Endnotes (cont'd)

9 16 CFR 681.2(d)(2)(i)-(iv).

10 16 CFR 681.2(f).

11 *See supra* note 2 at 63773-63774 (Appendix A to Part 681 – Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation and Supplement A to Appendix A).

12 *See supra* note 2 at 63728.

13 16 CFR 681.2(e).

14 16 CFR 681.2(e)(1)-(4).

15 16 CFR 681.2(e)(4).

16 *See supra* note 2 at 63773-74.

17 16 CFR 681.2(c).

18 16 CFR 681.2(c)(1)-(3).

19 16 CFR 681.3.

20 16 CFR 681.3(c).

21 16 CFR 681.3(e).

22 16 CFR 681.3(d).

23 A "notice of address discrepancy" means "a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer." 16 CFR 681.1(b).

24 16 CFR 681.1(c)(1).

25 *See supra* note 2 at 63736 (it is important for a user to form a reasonable belief that the consumer report relates to the consumer about whom it has requested the report both in the connection with the opening of an account and in other circumstances when the user already has a relationship with the consumer, such as when the consumer applies for an increased credit line).

26 16 CFR 681.1(c)(2)(ii).

27 31 CFR 103.121.

28 16 CFR 681.1(c)(2)(i)(A)-(C).

29 *See supra* note 2 at 63737.

30 *See id.*

31 *See supra* note 2 at 63737; *see also* 31 CFR 103.121(b)(2)(iii).

32 *See supra* note 2 at 683737.

33 16 CFR 681.1(d)(1).

34 16 CFR 681.1(d)(2)(i)-(iv).