

FDIC Approves Final Rules from FACTA

2007-10-23

On October 16, 2007, the Federal Deposit Insurance Corp. (FDIC) approved final rules implementing the affiliate marketing restrictions and identity theft prevention requirements from the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The Federal Trade Commission issued similar rules on October 23, 2007, and the other federal banking agencies and the Securities and Exchange Commission are expected to follow suit in the near future.

Affiliate Marketing Rule

The affiliate marketing rule, required under section 214 of the FACTA, prohibits covered institutions from using "eligibility information" received from an affiliate to make marketing solicitations to consumers, unless the consumers are given "clear and conspicuous" notice as well as a reasonable opportunity and a reasonable and simple method to opt out of such marketing.^[i]

What type of information is covered under the new rule? The rule applies to all "eligibility information," which is defined to include information the communication of which would constitute a "consumer report" under the Fair Credit Reporting Act (FCRA) **as well as** material that would otherwise be subject to exceptions from the definition of consumer report, such as transaction and experience information and information covered by an affiliate sharing opt-out notice.

What marketing activities are covered? An opt-out notice is required if you receive eligibility information from an affiliate (including through a shared database), you use that information to identify which consumers or types of consumers should receive solicitations or to otherwise tailor solicitations to those consumers, and the consumer receives a solicitation as a result. Note that the source of the solicitation is immaterial. Thus, an opt-out notice would be required prior to using eligibility information an affiliate has placed into a shared database to create or tailor a list of consumers, even if the solicitation is actually sent on behalf of that affiliate by the affiliate with a pre-existing relationship.

Who must provide the opt-out? The opt-out notice must be provided by an affiliate that has or has previously had a pre-existing business relationship with the consumer.

When must an opt-out notice be provided? An opt-out notice must be provided before you use eligibility information received from an affiliate to make a solicitation for marketing purposes. If a

"continuing relationship" exists with the consumer, a single opt-out notice may be drafted to cover current and future relationships and transactions with you and your affiliates.^[ii] In other situations (i.e., isolated transactions), an opt-out notice will only apply to information received in connection with that transaction.

What is the duration of an opt-out election? If a consumer elects to opt out, the opt-out must be effective for a period of at least five years, unless revoked by the consumer in writing.

Are there any exceptions to when an opt-out notice is required? Yes. The rule does not apply to the use of eligibility information received from an affiliate in a number of circumstances, including using the information to: (i) market to consumers with whom you have a pre-existing business relationship;^[iii] (ii) perform services on behalf of an affiliate; and (iii) respond to consumer communications regarding products or services or requests for solicitations.

What information must the opt-out include? The opt-out notice must disclose: (i) the identity of the affiliate(s) providing the notice; (ii) a list of affiliates or types of affiliates covered by the opt-out notice; (iii) the types of eligibility information that may be used to make solicitations; (iv) that the consumer may elect to limit such use of eligibility information for a renewable period of at least five years; (v) and that consumers who have previously opted out do not need to act until they receive a renewal notice. The opt-out notice must also include a "reasonable and simple" opt-out method. Model notices are provided in 12 C.F.R. part 334, Appendix A.

Does this mean I have to send my GLB privacy notice on a new schedule this year? No. Institutions are not required to comply with these rules until October 1, 2008. Further, there is no requirement that this opt-out notice be included in your GLB privacy notice. However, you may elect to consolidate this notice with your GLB privacy notice (or any other legally mandated notices), which may require that next year's privacy notice be sent earlier than usual to satisfy the October 1, 2008 deadline.

How long must I wait before using shared information for marketing? The customer must have a "reasonable opportunity" to opt out. For example, consumers should be given 30 days from the date the notice is mailed (or e-mailed if the consumer has consented), or 30 days from the date the consumer acknowledges receipt of a posted electronic notice. As a result, opt-out notices should be sent (or acknowledged) by September 1, 2008, in order to be effective by the mandatory compliance date. If the opt-out notice is included in a privacy policy, the consumer should be allowed a "reasonable period of time" in the same manner as the opt-out under that privacy notice.

Does this opt-out opportunity apply to information shared in the past? No. The rule does not prohibit the use of eligibility information received from an affiliate prior to October 1, 2008. This includes information that an affiliate places into a shared database prior to that date, even if you do not actually access the information until a later date.

What if I want to market on behalf of my affiliate? The rule allows so-called "constructive sharing," permitting an entity to use its own eligibility information to market an affiliate's products and services. However, it is important to note that providing certain informational material may trigger additional regulatory obligations under state law (i.e., insurance or mortgage lending limitations on

solicitation).

Are there any restrictions on my ability to share with affiliates for other purposes? This opt-out relates to the **use** of information by an affiliate and does not limit an institution's obligation to comply with the affiliate sharing notice and opt-out provisions of FCRA § 603(d)(2)(A)(iii) where applicable.

Identify Theft Prevention Measures

The FDIC also published a final rule implementing sections 114 and 315 of FACTA.[iv] The rule sets forth guidelines for the creation and maintenance of an Identity Theft Prevention Program(Program) as required by sections 114 of FACTA. The rule also provides guidelines for processing change-of-address requests for debit and credit card issuers. Collectively, these guidelines are referred to as the "Red Flag Regulations." Additionally, the rule sets out requirements related to address discrepancies in consumer reports. The mandatory compliance date for these rules and guidelines is November 1, 2008.

Identity Theft Prevention Program

What are the requirements for the Program? Financial institutions and creditors must adopt a written Program designed to detect, prevent and mitigate identity theft in connection with new or existing covered accounts. It must include reasonable policies and procedures to: identify and incorporate relevant red flags; provide for appropriate responses to red flags to prevent and mitigate identity theft; and ensure that the program is periodically updated.

Are there specific prescriptions for the Program? No. The rule adopts a risk-based approach similar to the Information Security Standards, requiring that the Program be "appropriate to the size and complexity of the institution and the nature and scope of its activities."

What accounts is the Program required to address? The rule applies to all "covered accounts," defined to include both accounts that are primarily for personal, family or household purposes and all other accounts determined to pose a "reasonably foreseeable risk" to customers or the safety and soundness of the financial institution or creditor.

Address Verification

When am I required to verify change of address information? Card issuers are required to verify change of address information whenever a consumer requests additional or replacement cards within 30 days of submitting a change-of-address notification.

How can I verify address information? You may verify this information by notifying the cardholder at the cardholder's former address and providing an opportunity to respond. Alternatively, you may use any other method agreed upon by the cardholder or as set forth in your Program.

Do I have to wait until I receive a request for additional or replacement cards? No. You may also satisfy this requirement by verifying the address each time you receive a change-of-address notification.

Consumer Reporting Agency (CRA) Address Discrepancies

When do I receive an address discrepancy notification? Under Section 315 of FACTA, nationwide consumer reporting agencies are required to notify you if the address you provide in your request "substantially differs" from the address in the CRA's file.

Am I required to do anything before I receive an address discrepancy notification? You are required to develop and implement reasonable policies and procedures designed to allow you to form a "reasonable belief" that a consumer report relates to the consumer about whom you requested the report.

How can I form such a "reasonable belief"? You should either verify the information directly with the consumer or compare the information with information from your records or third-party sources, or information obtained under the Customer Identification Program rules.

Am I required to do anything with verified information? You are also required to develop and implement reasonable policies and procedures designed to provide the CRA with "reasonably verified address information" on consumers with whom you establish a continuing relationship if you otherwise routinely furnish information to that CRA.

[i] According to the draft *Federal Register* notice released by the FDIC, this rule will be codified as follows in the CFR: 12 CFR Part 41 (Office of the Comptroller of the Currency); 12 CFR Part 222 (Federal Reserve System); 12 CFR Part 334 (FDIC); 12 CFR Part 571 (Office of Thrift Supervision); and 12 CFR Part 717 (National Credit Union Administration).

According to the draft notice released by the FDIC, this rule will be codified as follows in the CFR: 12 CFR Part 41 (Office of the Comptroller of the Currency); 12 CFR Part 222 (Federal Reserve System); 12 CFR Part 334 (FDIC); 12 CFR Part 571 (Office of Thrift Supervision); and 12 CFR Part 717 (National Credit Union Administration).] According to the draft notice released by the FDIC, this rule will be codified as follows in the CFR: 12 CFR Part 41 (Office of the Comptroller of the Currency); 12 CFR Part 222 (Federal Reserve System); 12 CFR Part 334 (FDIC); 12 CFR Part 571 (Office of Thrift Supervision); and 12 CFR Part 717 (National Credit Union Administration).

[ii] However, a new opt-out notice would be required if a consumer terminates all continuing relationships with you and your affiliates and subsequently establishes a new continuing relationship.

[iii] A "pre-existing business relationship" is defined to include an ongoing financial contract with the consumer, a transaction (either financial or for goods or services) with the consumer in the last 18 months or an inquiry or application by the consumer regarding a product or service in the last three months.

[iv] According to the draft *Federal Register* notice released by the FDIC, this rule will be codified as follows in the CFR: 12 CFR Part 41 (Office of the Comptroller of the Currency); 12 CFR Part 222 (Federal Reserve System); 12 CFR Parts 334 and 364 (FDIC); 12 CFR Part 571 (Office of Thrift Supervision); 12 CFR Part 717 (National Credit Union Administration); and 16 CFR Part 681 (Federal Trade Commission).

(Program) as required by section 114 of FACTA. The rule also provides guidelines for processing change-of-address requests for debit and credit card issuers. Collectively, these guidelines are referred to as the "Red Flag Regulations." Additionally, the rule sets out requirements related to address discrepancies in consumer reports. The mandatory compliance date for these rules and guidelines is November 1, 2008.