

FACTA Red Flag, Address Discrepancy and Information Sharing Rules Compliance – Hitting October/November 2008 Compliance Deadlines

INTRODUCTION

In October of last year, joint-agency rules were published on the Fair and Accurate Credit Transactions Act (FACTA) aimed at, among other things, preventing identity theft, ensuring proper use of consumer credit information, and imposing new guidelines and requirements for affiliate information sharing. This advisory addresses three of those rules, those applying to affiliate information sharing, red flag, and notice of address discrepancy issues, all three of which call for compliance by October or November. (See 16 CFR §§ 680, 681 and 698). It also includes strategies for ensuring you are on track for compliance by this fall.

AFFILIATE MARKETING RULE – OCTOBER 1, 2008

What's Required?

The Affiliate Marketing Rule prohibits businesses from using “eligibility information” received from an “affiliate” to “make a solicitation” for credit, insurance, or for employment purposes *unless* the consumer has received a notice of such use and reasonable/constructive opportunity to opt out, or unless the soliciting company has a pre-existing business relationship with the customer (*i.e.*, within 18 months since last transaction, or within 3 months of an inquiry).

“*Affiliate*” means companies related by common ownership/corporate control.

“*Eligibility Information*” means information that qualifies as a consumer report and transaction/experience information with the affiliate if such information is to be used to determine the consumer’s eligibility for credit, insurance, or employment. [Does not include aggregated, anonymous information].

“*Makes a solicitation*” means to use eligibility information from an affiliate to (a) identify a consumer/type of consumer who will receive an offer, (b) establish criteria to make consumer offers, or (c) decide which products/services to market, and use the resulting information for solicitation.

“*Solicitation*” means proactively marketing a product or service to a consumer based on Eligibility Information obtained from an affiliate.

No general opt-out is required. The rule only applies when using consumer Eligibility Information to determine eligibility for and proactively market credit or insurance, or for employment purposes.

What to Do?

To ensure proper notices/opt-outs are in place by October, work with counsel to:

- Review all current sharing practices and associated consumer-facing disclosures to identify where, if any place, a revised notice and/or opt-out is required.
- To the extent revised practices are warranted, determine what technical and non-technical changes are required in order to meet the October compliance deadline.

RED FLAG RULE – NOVEMBER 1, 2008

What's Required?

The Red Flag Rule applies to “financial institutions” and “creditors” (both broadly defined) and requires a comprehensive written program designed to prevent, detect, and mitigate ID theft if the business offers a “covered account.” “Covered account” is defined to include: (i) consumer accounts that have multiple pay-

ments/transactions (e.g., cell phone account), or (ii) other types of accounts that carry a reasonably-foreseeable risk to the customers/business from identity theft. The program must be approved by the appropriate oversight function of the business implementing it (e.g., board of directors), which function must also accept continuing compliance oversight, including managing employee training and monitoring internal and vendor/supplier adherence to stated policies.

What to Do?

In order to ensure you have a comprehensive ID theft program in place by November, work with counsel to:

- Identify the team responsible for developing and implementing the program. The team should include at a minimum representatives from sales, credit, operations, fraud, collections, customer service, training, and legal functions.
- Pull and review all *existing* fraud/ID theft-related policies/procedures.
- Conduct a gap analysis of policies/procedures and, where necessary, draft new/modified/enhanced policies and procedures as needed.
- Develop a single-source combined set of program policies incorporating new and existing materials.
- Obtain board approval of the proposed unified program.
- On approval, conduct appropriate training and implementation per program guidelines.
- Audit and update the program as appropriate on a regular recurring basis.

ADDRESS DISCREPANCY – NOVEMBER 1, 2008

What's Required?

The Address Discrepancy Rule requires covered businesses that use consumer reports to develop and implement reasonable policies and procedures for how to handle

consumer credit information subject to a notice of address discrepancy from a consumer reporting agency.

In this context, “notice of address discrepancy” means a notice sent to a business by a consumer reporting agency (CRA) informing the business of a substantial difference between the address the business provided to the CRA in order to request a consumer report and the address(es) in the CRA’s file for that consumer.

What to Do?

In order to develop a comprehensive address discrepancy program by November, work with counsel to:

- Identify existing policies/procedures that enable your business to link information on a consumer with a corresponding notice of address discrepancy, and if no such capability exists, take steps to create appropriate technical links to match notices to the individuals they reference.
- Confirm or establish a process to confirm, as condition of using a consumer report on an individual where a notice of address discrepancy is received, that the consumer report obtained relates to the consumer on who it was requested.

For more information about this Client Advisory, please contact:

JOEL E. HEWER, ESQ.

Co-Chair, Consumer Financial Services Group

202-342-8520

jhewer@kelleydrye.com

DONNA L. WILSON, ESQ.

Co-Chair, Consumer Financial Services Group

202-342-8475

dwilson@kelleydrye.com