



# ALERT

For Clients and Friends of DREHER LANGER & TOMKIES L.L.P.  
October 23, 2007

## FTC ISSUES FINAL RULE IMPLEMENTING FACTA AFFILIATE MARKETING PROVISION; OTHER RULES EXPECTED SHORTLY

The Federal Trade Commission (FTC) has issued a final rule implementing Section 214 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which regulates use of information received from an affiliate for marketing purposes. Several other federal agencies, including the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Board), the Federal Deposit Insurance Corporation (FDIC) and the Office of Thrift Supervision (OTS), are expected to approved final rules implementing Sections 214 shortly. A summary of the FTC's final rules follows.

The agencies also are expected to issue final rules implementing both Section 114 and Section 315 of the FACTA, which deal with identity theft "red flags" and address discrepancies, in the near future.

The FDIC made available advance copies of both rules as part of the agenda for its October 16, 2007 Board of Directors' meeting, along with memoranda recommending that the Board approve the rules. The summary of the red flag/address discrepancy regulations below is based on the advance copy of those rules.

### Affiliate Marketing

Section 214 of the FACTA (i) added a new section (15 U.S.C. § 1681s-3) to the Fair Credit Reporting Act regarding affiliate sharing and (ii) required the federal banking agencies to issue rules implementing Section 214 in coordination with one another.

Proposed regulations were issued in June and July of 2004. See OCC, Board, FDIC, OTS and NCUA Notice of Proposed Rule Making: Fair Credit Reporting Affiliate Marketing Regulations, 69 Fed. Reg. 42502 (July 15, 2004); FTC Proposed Rule: Affiliate Marketing Rule, 69 Fed. Reg. 33324 (June 15, 2004). The agencies made many changes to the proposed rules in response to comments received, although the basic elements of the rules are

substantially similar. Key changes include a revised approach to the scope of the opt-out and the contents of the opt-out notice and an expansion of the number of model forms.

The final rule sets out three conditions that must be met before an affiliate may use "eligibility information" (defined to include transaction and experience information and other information, such as data gathered from consumer reports or applications) for marketing purposes: (i) an affected consumer must receive clear, conspicuous, concise, written notice that the affiliate may use shared eligibility information to make solicitations to the consumer, (ii) the consumer must be provided with a reasonable opportunity and a reasonable and simple method to direct the affiliate not to use the consumer's eligibility information for this purpose and (iii) the consumer must not have exercised the consumer's opportunity to opt out.

Under the final rule, an opt out must be valid for at least five years. After the opt-out period expires, an entity that has received eligibility information from an affiliate about a consumer who previously opted out may not solicit that consumer until the consumer has been given a renewal notice and a reasonable opportunity to opt out, and does not renew the opt-out.

The final rule sets out statutory exceptions to the notice and opt-out requirements as follows:

- Marketing to a consumer with whom an entity has a pre-existing business relationship;
- Facilitating communications to an individual for whose benefit an entity has provided employee benefit or other services;
- Performing services on behalf of an affiliate, except for marketing on behalf of an affiliate if the affiliate would not be permitted to do so;
- Responding to a communication about products or services initiated by the consumer;
- Responding to an authorization or request by the consumer to receive solicitations; or
- Complying with any provision of state insurance laws pertaining to unfair discrimination in any state in which the entity is lawfully doing business.

The final rules implementing Section 214 will be effective January 1, 2008, with a mandatory compliance date of October 1, 2008.

Darrell L. Dreher  
ddreher@dtlaw.com

Michael C. Tomkies  
mtomkies@dtlaw.com

Margaret M. Stolar  
mstolar@dtlaw.com

Robin R. De Leo  
robin@dreher-la.com

Charles V. Gall  
cgall@dtlaw.com

Susan L. Ostrander  
sostrander@dtlaw.com

Kathleen L. Caress  
kcaress@dtlaw.com

Robert J. Kapitan  
r.kapitan@worldnet.att.net

Vanessa A. Nelson  
vnelson@dtlaw.com

## DREHER LANGER & TOMKIES L.L.P.

Attorneys at Law

2250 Huntington Center, 41 S. High Street  
Columbus, Ohio 43215

Telephone: (614) 628-8000 / Facsimile: (614) 628-1600  
www.dtlaw.com

Jeffrey I. Langer  
jlanger@dtlaw.com

Judith M. Scheiderer  
jscheiderer@dtlaw.com

Elizabeth L. Anstaett  
eanstaett@dtlaw.com

This ALERT is provided as a complimentary service for Clients and Friends of the Firm. To decline future ALERTS, please contact Mary Kirkham at (614) 628-1613 or [mkirkham@dtlaw.com](mailto:mkirkham@dtlaw.com). This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

### Red Flags and Address Discrepancies

Section 114 of the FACTA requires the agencies to jointly issue guidelines for use by financial institutions and creditors regarding identity theft. In developing the guidelines, the agencies were instructed to identify patterns, practices and specific forms of activity that indicate the possible existence of identity theft and consider requiring financial institutions and creditors to follow reasonable policies and procedures that provide for notice to a consumer when a transaction occurs with an inactive account. Section 114 also directs the agencies to prescribe regulations to ensure that card issuers do not issue additional or replacement cards without verifying certain change of address requests.

Section 315 of the FACTA requires the agencies to jointly issue regulations providing guidance regarding policies and procedures that users of consumer reports can use when they receive notice from a consumer reporting agency (CRA) of a substantial difference between the consumer address used to request the consumer report and the address for that consumer in the CRA's file.

Proposed rules for Sections 114 and 315 were issued in July 2006. See OCC, Board, FDIC, OTS, National Credit Union Administration (NCUA) and FTC Proposed Rule: Identity Theft Red Flags and Address Discrepancies Under the FACTA. 71 Fed. Reg. 40786 (July 18, 2006). The agencies modified the proposed rules and guidelines in response to comments received, primarily to provide greater flexibility and guidance to financial institutions and creditors.

As required, the final rules implementing Sections 114 and 315 regulate (i) identity theft prevention programs, (ii) change of address requests for card issuers and (iii) verification of consumer identity upon notice of address discrepancy. Items (i) and (ii) collectively are called the "Red Flag Regulations."

Under the final Red Flag Regulations, a financial institution or creditor must have a written Identity Theft Prevention Program for all accounts primarily for personal, family or household purposes and for all other accounts in which the financial institution or creditor determines there is a reasonably foreseeable risk of identity theft. The program must be designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The final Red Flag Regulations adopt a flexible risk-based approach similar to the approach used in the Interagency Guidelines Establishing Information Security Standards issued by the federal banking agencies and the Standards for Safeguarding Customer Information issued by the FTC. The Identity Theft Prevention Program must be appropriate to the size and complexity of the institution and the nature and scope of its activities and be flexible enough to address changing identity theft risks as they arise.

The final rules list four basic elements that must be included in the program, including "reasonable policies and procedures" to:

- Identify relevant red flags for covered accounts and incorporate those red flags into the program;
- Detect red flags that have been incorporated;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The final rules also list certain steps that financial institutions and creditors must take regarding the program, including obtaining approval of the initial written program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the program, training staff and overseeing service provider arrangements. Appendix J to the final rules contains detailed guidelines on how to formulate and maintain a program that satisfies the regulatory requirements to detect, prevent and mitigate identity theft.

Regarding change of address requests, the Red Flag Regulations provide that a credit or debit card issuer who receives notification of a change of address for an account, and within a short period of time afterwards (during at least the first 30 days after it receives such notification) receives a request for an additional or replacement card for the same account, may not honor the request and issue such a card, unless it assesses the validity of the change of address request in at least one of three ways:

- Notifying the cardholder of the request at the cardholder's former address and providing to the cardholder a means of promptly reporting incorrect address changes;
- Notifying the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or
- Using other means of assessing the validity of the change of address, in accordance with the policies and procedures that the card issuer has established pursuant to the Red Flag Regulations.

The final rules clarify that a card issuer may satisfy the requirements by validating an address whenever it receives an address change notification, even if that notification arrives before it receives a request for an additional or replacement card.

Regarding address discrepancies, the final rules provide that a user must develop and implement reasonable policies and procedures designed to enable it to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when the user receives a notice of address discrepancy. If a user cannot establish a reasonable belief that the consumer report relates to the consumer about whom it has requested the report, the agencies expect that the user will not use that report.

The final rules also require that a user develop and implement reasonable policies and procedures for furnishing an address for the consumer to the CRA that the user has reasonably confirmed is accurate, when the following three conditions are present: (i) the user forms a reasonable belief that a consumer report relates to the consumer about whom it requested the report, (ii) the user "establishes" a continuing relationship with the consumer and (iii) the user regularly and in the ordinary course of business furnishes information to the CRA.

The final rules implementing Sections 114 and 315 will be effective the first day of the calendar quarter after publication in the Federal Register, with a mandatory compliance date of November 1, 2008. □

✧ *Elizabeth Anstaett and Vanessa Nelson*