



November 2007

ALBANY
AMSTERDAM
ATLANTA
BOCA RATON
BOSTON
CHICAGO
DALLAS
DELAWARE
DENVER
FORT LAUDERDALE
HOUSTON
LAS VEGAS
LOS ANGELES
MIAMI
NEW JERSEY
NEW YORK
ORANGE COUNTY
ORLANDO
PHILADELPHIA
PHOENIX
SACRAMENTO
SILICON VALLEY
TALLAHASSEE
TAMPA
TOKYO
TYSONS CORNER
WASHINGTON, D.C.
WEST PALM BEACH
ZURICH

*Strategic Alliances with
Independent Law Firms*

BRUSSELS
LONDON
MILAN
ROME
TOKYO

It's Official – 'Red Flag' Identity Theft Programs Must Be In Place By 2008

On October 31, 2007, the federal banking agencies, together with the U.S. Department of the Treasury and the Federal Trade Commission, issued final "Red Flag" regulations (the "Red Flag Regulations") enacting Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). The Red Flag Regulations require all financial institutions and providers of credit to adopt "Red Flag" identity theft policies and programs by no later than November 1, 2008. Accordingly, senior management and compliance officers of affected financial institutions and creditors should now begin the process of (i) assessing their identity theft risk profiles, (ii) adopting and testing appropriate policies and procedures that comply with the Red Flag Regulations, and (iii) training their employees to ensure that those policies and procedures are implemented effectively.

Are You Covered?

These Red Flag Regulations are mandatory for all "financial institutions" – i.e., banks, thrifts, mortgage lenders, credit unions, their non-functionally regulated operating subsidiaries, U.S. branches and agencies of foreign banks, U.S. commercial lending companies of foreign banks – and "creditors," or any person or business who arranges for the extension, renewal, or continuation of credit. Thus, in addition to banking institutions, retailers, utilities, car dealers and many other businesses are subject to this regulation.

The Red Flag Regulations

The Red Flag Regulations require each financial institution and creditor that holds any consumer account – or any other account for which there is a reasonably foreseeable risk of identity theft – to develop and implement an "Identity Theft Prevention Program" for combating identity theft in connection with new and existing accounts. The program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and must enable a financial institution or creditor to:

- 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;
- 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 is updated periodically to reflect changes and risks from identity theft.

The regulations contain guidelines that identify no less than 31 patterns, practices and specific forms of activities that indicate possible risk of identity theft. To promote flexibility and responsiveness to the changing nature of identity theft, however, the regulations state that covered entities must include in their programs relevant red flags from applicable supervisory guidance, their own experience, and methods that the entity has identified that reflect changes in identity theft risk. This effectively means that financial institutions and creditors should regularly update their Red Flag policies and procedures to adapt them to evolving methods of identity theft.

Which Accounts Are Targeted?

The Red Flag Regulations define customer as a person that has a covered account with the financial institution or creditor. Generally, a covered account is one 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.

But the Red Flag Regulations also define a covered account as “any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity risk, including financial, operational, compliance, reputation, or litigation risk.” In effect, then, this definition may require financial institutions to include business identity theft as part of their programs.

Address Changes

The Red Flag Regulations also 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 thereafter (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 a change of address request in at least one of three ways:

- notifying the cardholder of his or her purported request at the cardholder’s former address and provide to the cardholder a means of reporting incorrect address changes;
- notifying the cardholder of his or her purported request by any other means of communication that the cardholder and the cardholder have previously agreed to use; or
- using other means of assessing the validity of the purported change of address, in accordance with the policies and procedures that the card issuer has established pursuant to the Red Flag Regulations.

Address Discrepancy Regulations

The Red Flag Regulations also implement Section 315 of the FACTA, which requires that a nationwide consumer reporting agency, when providing consumer reports to requesting user, notify the requesting user of the existence of a discrepancy if the address provided by the user in its request “substantially



differs" from the address the consumer reporting agency has in the consumer's file. A user must develop and implement reasonable policies and procedures that are designed to enable 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. These must apply both in 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. If a user cannot establish a reasonable belief that the consumer report relates to the consumer about whom it has requested the report, the enforcing agencies expect that the user will not use that report. The final rule does, however, provide examples that a user may employ to form that reasonable belief.

Effective Date

The final rules and guidelines will be effective on the first day of the calendar quarter after publication in the Federal Register, or likely January 1, 2008. More important, the mandatory compliance date for rules and guidelines will be November 1, 2008.

GT Can Help

Greenberg Traurig's Financial Institution and Data Privacy professionals can help you:

- conduct your risk assessment and design and develop your Red Flag Program and Policy, including employee training;
- advise on your duty to detect, prevent, and mitigate identity theft;
- analyze and prepare vendor agreements that comply with your Red Flag duties; and
- advise Board and Senior Management on their responsibilities and plans.

For more information, please contact a member of our Financial Institution Practice or our Privacy and Data Security Task Force.



This *GT Alert* was prepared by Luis Salazar and Carl Fornaris. Questions about this *Alert* can be directed to:

- Luis Salazar at 305.579.0751 (salazarl@gtlaw.com)
- Carl Fornaris at 305.579.0626 (fornarisc@gtlaw.com)
- Gil Rudolph at 602.445.8206 (rudolphg@gtlaw.com)

Albany 518.689.1400	Houston 713.374.3500	Sacramento 916.442.1111
Amsterdam + 31 20 301 7300	Las Vegas 702.792.3773	Silicon Valley 650.328.8500
Atlanta 678.553.2100	Los Angeles 310.586.7700	Tallahassee 850.222.6891
Boca Raton 561.955.7600	Miami 305.579.0500	Tampa 813.318.5700
Boston 617.310.6000	New Jersey 973.360.7900	Tokyo + 81 3 3264 0671
Chicago 312.456.8400	New York 212.801.9200	Tysons Corner 703.749.1300
Dallas 214.665.3600	Orange County 714.708.6500	Washington, D.C. 202.331.3100
Delaware 302.661.7000	Orlando 407.420.1000	West Palm Beach 561.650.7900
Denver 303.572.6500	Philadelphia 215.988.7800	Zurich + 41 44 224 22 44
Fort Lauderdale 954.765.0500	Phoenix 602.445.8000	

This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ©2007 Greenberg Traurig, LLP. All rights reserved.