PROSKAUER ROSE LLP®

Client Alert

A report
for clients
and friends
of the Firm

March 2008

Feds Put Companies on Notice: Be Ready to Detect and Respond to Red Flags of Identity Theft

According to new regulations published by the Federal Trade Commission ("FTC") and the federal banking agencies, covered companies that hold any customer accounts must implement identity theft prevention programs that identify and detect "Red Flags" signaling possible identity theft. Under these regulations, companies establishing such programs must create policies and procedures not only to recognize and detect Red Flags, but also to respond to Red Flags by preventing or mitigating potential identity theft. Furthermore, companies must develop reasonable policies and procedures to verify the identity of a customer opening an account, and must also periodically update their identity theft programs. The rules went into effect on January 1, 2008, and businesses must comply by November 1, 2008.

Scope of the Red Flags Rule

Federal regulators issued the final Red Flags rules pursuant to Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which requires these agencies to identify patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft. The final rules apply to all financial institutions and creditors that hold or maintain "covered accounts" defined as "(1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft." Under the rules, financial institutions are defined in accordance with the Fair Credit Reporting Act and include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. "Creditors are defined as persons or businesses that arrange for the extension, renewal, or continuation of credit," and thus encompass a wide range of entities, including car dealers, utilities, as well as third-party debt collectors.

Given the broad reach of the regulations, the agencies gave financial institutions and creditors significant flexibility to determine which Red Flags are relevant to detect identity theft. According to the final rules, businesses "may tailor the Red Flags it chooses for its Program to its own operations. A financial institution or creditor will not need to justify to an Agency its failure to include in the Program a specific Red Flag from the list of examples. However, a covered entity will have to account for the overall effectiveness of a Program that is appropriate to its size and complexity and the nature and scope of its activities." Additionally, the rules suggest that companies acquire approval of the program from the board of directors or a committee of the board, as well as exercise oversight of the implementation of the program, training staff and employees, and service provider arrangements.

Examples of Red Flags

To assist financial institutions and creditors in choosing which Red Flags to identify, the agencies provide an extensive list of possible Red Flags that may require further action when they come to the attention of a company, consisting, in part, of the following:

- A fraud alert, credit freeze, or address discrepancy is included with a consumer report or provided by a credit reporting agency.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.

- Documents, applications, or photo identification provided appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.

- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

- Personal identifying information provided is inconsistent when compared to other personal identifying information on file with the financial institution or creditor or provided by the customer (i.e., there is a lack of correlation between the SSN range and date of birth), or otherwise inconsistent when compared against external information sources used by the financial institution or creditor.

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.

- The SSN, address or telephone provided is the same as that submitted by other customers or by an unusually large number of other persons opening accounts.

- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- A covered account is used in a manner that is not consistent with established patterns of activity on the account.

As stated above, businesses must also implement customer verification procedures. Financial institutions subject to the existing Customer Identification Program ("CIP") rules promulgated under Section 326 of the USA PATRIOT Act may satisfy the FACTA customer verification procedures by complying with CIP. Nevertheless, "[t]he Agencies expect all financial institutions and creditors to evaluate the adequacy of existing policies and procedures and to develop and implement risk-based policies and procedures that detect Red Flags in an effective and comprehensive manner."

Change of Address Requests

Additionally, the federal agencies published rules, which were required under Section 114 of FACTA, regarding the issuance of new credit or debit cards coming directly after a change of address request. Under these rules, issuers of credit and debit cards must develop reasonable policies and procedures to validate a customer's change of address request placed shortly before – within at least 30 days – a request for an additional or replacement card. According to the rules, "The card issuer may not issue the card unless it: (1) notifies the cardholder of the request at the cardholder's former address and provides the cardholder with a means to promptly report an incorrect address; (2) notifies the cardholder of the address change request by another means of communication previously agreed to by the issuer and the cardholder; or (3) uses other means of evaluating the validity of the address change in accordance with the reasonable policies and procedures established by the card issuer to comply with the joint regulations described earlier regarding identity theft."

Address Discrepancy Notices

The final rules also implement Section 315 of FACTA, which compels users of credit reports to establish policies and procedures to apply if they receive from a consumer reporting agency a notice of a substantial difference between the consumer's address provided by the user in requesting the report and the address the consumer reporting agency has in its file. Such measures include "verifying the address with the person to whom the consumer report pertains, reviewing its own records of the address provided to request the consumer report, or verifying the address through third-party sources."

BOCA RATON • BOSTON • LONDON

LOS ANGELES • NEW ORLEANS • NEW YORK • NEWARK

PARIS • SÃO PAULO • WASHINGTON, D.C.

Client Alert

Proskauer's litigation department consistently addresses complex litigation matters generated by the global business economy. The department has over 240 lawyers practicing from the Firm's offices in New York City, Los Angeles, Washington D.C., Boston, Boca Raton, Newark, New Orleans and Paris. The Firm practices in a wide range of forums across the nation and abroad, including federal and state courts, administrative and regulatory agencies and national and international arbitral tribunals.

For more information please contact:

Tanya L. Forsheit
310.284.4508 – tforsheit@proskauer.com

Grégoire Goussu
33.1.53.05.60.11 – ggoussu@proskauer.com

Kristen J. Mathews
212.969.3265 – kmathews@proskauer.com

Jeffrey D. Neuburger
212.969.3075 – jneuburger@proskauer.com

Proskauer Rose is an international law firm that handles a full spectrum of legal issues worldwide.

You can also visit our Website at **www.proskauer.com**