

SCHWARTZ & BALLEN LLP

1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465

(202) 776-0700

FACSIMILE
(202) 776-0720

www.schwartzandballen.com

M E M O R A N D U M

October 18, 2007

To Our Clients and Friends

Re: FACT Act: Identity Theft Red Flags and Address Discrepancies

The Federal Deposit Insurance Corporation has adopted a final rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”) regarding identity theft red flags for financial institutions and procedures that users of consumer reports should use in the event they receive notices from consumer reporting agencies (“CRAs”) of address discrepancies. It is anticipated that the Federal Reserve Board, Office of the Comptroller of the Currency, Office of Thrift Supervision, National Credit Union Administration and Federal Trade Commission (the “Agencies”) will adopt identical rules in the near future. Institutions are required to comply with the regulations by November 1, 2008.

RED FLAG GUIDELINES

Section 114 of the FACT Act requires the Agencies to jointly issue guidelines identifying patterns, practices and specific forms of activities that indicate the possible existence of identity theft (“Red Flags”). The Agencies must also require financial institutions and creditors to establish reasonable policies and procedures regarding identity theft with respect to account holders and customers.

The Red Flags rule requires financial institutions and creditors that offer “covered accounts” to implement a written program which contains reasonable policies and procedures to address the risk of identity theft and to identify accounts where identity theft is most likely to occur. A covered account is (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions, or (2) an account for which there is a reasonably foreseeable risk to customers or to the safety or soundness of the institution or of the creditor from identity theft. The Red Flags guidelines adopted

SCHWARTZ & BALLEN LLP

along with the rule provide specific examples of the types of activities that may indicate the possible risk of identity theft.

An institution's program must be designed to detect, prevent and mitigate identity theft in connection with a covered account and must be tailored to the institution's size, complexity and nature of its activities. The program must also contain reasonable policies and procedures that cover the following four elements:

- Identify relevant Red Flags for covered accounts and incorporate them 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
- Ensure the program is updated periodically

The program is to be approved by the institution's board of directors or an appropriate board committee. Guidelines have been adopted for institutions to consider when developing policies and procedures. In addition, examples of Red Flags are provided as a supplement to the guidelines.

CARDHOLDER CHANGE OF ADDRESS

Credit and debit card issuers will be required to implement policies and procedures to assess the validity of a change of address request when it is followed by a request for an additional or replacement card within a short period of time (*e.g.*, 30 days). A card issuer may not issue an additional or replacement card unless it notifies the cardholder of the request at the cardholder's former address, notifies the cardholder by other means previously agreed to by the cardholder or uses other means of assessing the validity of the change of address. A card issuer may also satisfy the requirements by validating an address whenever it receives an address change notification even if the notification arrives before it receives a request for an additional or replacement card.

RECONCILING ADDRESS DISCREPANCIES

The final regulation also requires a user of consumer reports to develop and implement reasonable policies and procedures 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 notice from the CRA that the address for the consumer provided by the user differs substantially from the address in the consumer's file at the CRA. A user that applies the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules under the USA PATRIOT Act will satisfy this requirement. If the user cannot establish a reasonable

SCHWARTZ & BALLEEN LLP

belief that the consumer report relates to the consumer about whom it has requested the report, it should not use the report.

A copy of the final rule can be found on our web site at http://www.schwartzandballen.com/whats_new.html.

If you have any questions, please call Gilbert Schwartz, Robert Ballen, Tom Fox or Heidi Wicker at (202) 776-0700.