Provident BANK

September 15, 2006

By electronic delivery

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

RE: RIN 3064-AD00

Dear Mr. Feldman:

Provident Bank of Maryland ("Provident") is pleased to provide this comment letter to the Federal Deposit Insurance Corporation (FDIC) in response to the inter-agency (the "Agencies") proposed guidelines and regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

Provident is a state-chartered, one-bank holding company with headquarters in Maryland. With $6.4 billion in assets, Provident serves individuals and businesses in the areas of Greater Baltimore, Greater Washington and Central Virginia through a network of over 150 offices in Maryland, Virginia, District of Columbia and Southern York County, Pennsylvania.

Comments:

1. As noted in the preamble to the subject proposal, Section 114 of the FACT Act broadly describes the elements that belong in the regulation and those that belong in the guidelines. We are concerned that the Agencies' approach to managing identity theft as set forth in the Red Flag Guidelines (Appendix J) will force financial institutions to look for ways to apply the same solution across all product types and account types. We believe that this will result in overwhelming inefficiencies and increased costs for compliance that will inevitably be passed to the consumer. We are concerned that the proposal will be construed to require that financial institutions develop systems to extract and record each type of incident and/or activity that is characterized as a red flag. This approach will pose significant challenges to financial institutions and to the vendors that supply software and services to those financial institutions, because of the sheer number of red flag types and the absence of mechanisms to track and identify such red

flags using existing systems applications. We recommend that the Agencies provide financial institutions with the flexibility of selecting only those red flag types that are appropriate to each institution's products, account types and past ID theft experience--without fear of regulatory criticism. We believe that the appropriate examination focus should be on the number of ID theft incidences recorded by the institution (as required by Appendix B, Section 364) and not on examiner discretion. In addition, financial institutions and their service vendors should be provided sufficient time before the compliance effective date to develop their ID theft programs in accordance with the guidelines. We request that the final compliance effective date be moved to June 2008.

2. We are particularly concerned about the broad definitions of "account" and "customer" that are described in the proposal. The expansion of these terms to include entities that are not presently covered (e.g., partnerships and corporations), will cause additional compliance burdens and uncertainty. For purposes of consistency, we recommend that these definitions be identical to those found in the Agencies' privacy regulations and information security standards.

3. We are also concerned about the undefined risks to "account holders" and "customers" that may identify a "possible incidence" of identity theft. Provident, like many institutions, currently uses several software systems and reports from consumer reporting agencies to monitor new and existing customer activity. Fraud alerts, address discrepancies and inconsistent patterns of customer account activity are reviewed closely, particularly within the first 90 days of account opening--the period when ID theft is most likely to occur. We also have systems in place to notify us if an account is closed at another institution for cause. If financial institutions are required to monitor for the "possible existence" of ID theft beyond the customer information and activity that is presently collected and evaluated, the development and the cost of creating such systems will be enormous. It will be no easy task to develop and implement an appropriate ID Theft Prevention Program, if institutions are required to create multiple "possible incidence" scenarios.

4. The proposal provides that a financial institution or creditor "must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft." We are concerned that this will have a chilling effect similar to that which the banking industry has experienced with the filing of Suspicious Activity Reports (SARs) under the Bank Secrecy Act rules. Financial institutions have found through examination experience that they must justify why SARs are not filed. We are most interested in preserving the "flexibility" inherent in the ID Theft regulation and we are concerned that the proposed guidelines will undercut that structure.

Conclusion

At Provident, we take great care to protect the security and confidentiality of our customer's personal financial data. We maintain systems, controls and procedures throughout the organization in many different formats to monitor for activity that may be evidence of ID theft. While we support the Agencies' efforts to address this growing problem, we strongly recommend that the final rules and guidelines provide sufficient flexibility to allow institutions to continue using the ID Theft tools and methods that are currently available and not require institutions to make major adjustments or acquisitions that will ultimately have a financial impact on customers.

Thank you for the opportunity to express our views with respect to this proposal.

Sincerely,

Thomas W. Bernoski
Provident Bank of Maryland
Senior Vice President and
Compliance Officer