MEMORANDUM TO: The Board of Directors

FROM: Sandra L. Thompson
Director
Division of Supervision and
Consumer Protection

Sara A. Kelsey
General Counsel

SUBJECT: Interagency Final Rule Regarding Identity Theft Red Flags and Address Discrepancies under Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003

RECOMMENDATION:

We recommend that the Board of Directors (Board) of the Federal Deposit Insurance Corporation (FDIC or Corporation) authorize the Executive Secretary to publish in the *Federal Register* a final rule jointly with the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission (collectively, the Agencies) to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

The rule would establish: (1) interagency regulations requiring financial institutions and creditors to develop and implement a written identity theft prevention program; (2) interagency guidelines describing factors that financial institutions and creditors should address in their programs' policies and procedures; (3) interagency regulations requiring credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances; and (4) interagency regulations addressing reasonable policies and procedures that a user of consumer reports should employ upon receiving a notice of address discrepancy from a consumer reporting agency.

We also recommend that the Board authorize the Executive Secretary and the General Counsel to make technical, nonsubstantive, or conforming changes to the text of the rule where necessary to ensure that the Agencies can jointly publish the rule, and to take such other actions and issue such other documents as they deem necessary or appropriate to fulfill the Board's objectives.

DISCUSSION:

1. *Background*. The guidelines and regulations are required by sections 114 and 315 of the FACT Act, which amend the Fair Credit Reporting Act (FCRA). Section 114 of the FACT Act requires the Agencies to jointly issue guidelines for use by financial institutions and creditors regarding identity theft. In developing the guidelines, the Agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft, and they must 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. In addition to the guidelines themselves, the Agencies must issue regulations requiring financial institutions and creditors to establish reasonable policies and procedures for implementing the guidelines. The Agencies also must issue regulations requiring credit and debit card issuers to assess the validity of change of address requests.

Section 315 of the FACT Act requires the Agencies to issue regulations providing guidance regarding policies and procedures that users of consumer reports shall use when they receive notice from a consumer reporting agency of a substantial difference between the consumer address used to request the consumer report and the address for that consumer in the consumer reporting agency's file. (The guidelines and regulations required by section 114 are referred to collectively as the Red Flag Regulations.)

2. Proposal. On July 18, 2006, the Agencies published a joint notice of proposed rulemaking (NPR) in the Federal Register, at 71 FR 40786, proposing rules and guidelines to implement section 114 and proposing rules to implement section 315 of the FACT Act.

Identity Theft Prevention Program

The Agencies proposed to implement section 114 through regulations requiring each financial institution and creditor to implement a written Identity Theft Prevention Program (Program) and setting forth certain requirements for that Program. The Agencies also proposed guidelines that identified 31 patterns, practices, and specific forms of activity that indicate a possible risk of identity theft (red flags). The proposed regulations required each financial institution and creditor to incorporate into its Program relevant red flags, including indicators from among those listed in the guidelines. To promote flexibility and responsiveness to the changing nature of identity theft, the proposed rule also stated that covered entities would need to include in their Programs relevant red flags from applicable supervisory guidance, their own experiences, and methods that the entity had identified that reflect changes in identity theft risks.

Change of Address Requests for Card Issuers

The proposal also required credit and debit card issuers to assess the validity of change of address requests. The rules related to this issue come into play when the card issuer receives a notice of change of address for an existing account, and within a short period of time (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. In these cases, the card issuer 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. The proposal required that, in accordance with the card issuer's reasonable policies and procedures, the card issuer must: (1) notify the cardholder of the request at the cardholder's former address and provide to the cardholder a means of promptly reporting incorrect address changes; (2) notify the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or (3) use other means of assessing the validity of the change of address, in accordance with the policies and procedures that the card issuer has established. These factors were taken directly from Section 114 of the FACT Act.

Verifying Consumer Identity Upon Notice of Address Discrepancy

In addition, the Agencies proposed joint regulations under section 315 that required a user of a consumer report to develop and implement reasonable policies and procedures for "verifying the identity of the consumer for whom it has obtained a consumer report" whenever it receives a notice of substantial address discrepancy from a consumer reporting agency. Under the proposal, these policies and procedures would need to be designed to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report, or determine that it cannot do so. Under the proposal, the user may reasonably confirm an address is accurate by 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, verifying the address through third-party sources, or using other reasonable means. This section provided that if a user employed the policies and procedures regarding identification and

verification set forth in the customer identification program (CIP) regulations implementing section 326 of the USA PATRIOT Act, it satisfied the requirement to have policies and procedures to verify the identity of the consumer. The proposal further provided that a user must develop and implement reasonable policies and procedures for furnishing to the consumer reporting agency an address for the consumer that the user has reasonably confirmed is accurate when certain conditions are satisfied.

3. Comments Received. The public comment period closed on September 18, 2006. The FDIC received 38 comments. The comments included 27 from financial institutions or financial institution holding companies, seven from financial institution trade associations, three from other business entities, and one from an intellectual property task force. The Agencies collectively received a total of 128 comments in response to the NPR (although many commenters sent copies of the same letter to each of the Agencies), including three comments from consumer groups.

With respect to the red flag regulations and guidelines most industry commenters asserted that the proposal was overly prescriptive, contained requirements beyond those mandated in the FACT Act, would be costly and burdensome to implement, and would complicate the existing efforts of financial institutions and creditors to detect and prevent identity theft. Some industry commenters asserted that the rulemaking was unnecessary because large businesses, such as banks and telecommunications companies, already are motivated to prevent identity theft and other forms of fraud in order to limit their own financial losses and are already doing most of what would be required by the proposal as a result of having to comply with the CIP rules and other existing requirements. Consumer groups maintained that the proposed regulations provided too much discretion to financial institutions and creditors. Some small financial institutions also expressed concern about the flexibility afforded by the proposal and stated that they preferred to have clearer, more structured guidance describing exactly how to develop and implement a Program and what they would need to do to achieve compliance.

Thirteen comment letters sent to the FDIC addressed the portion of the proposal concerning credit and debit card issuers who need to assess the validity of change of address requests followed shortly by a request for an additional or replacement card. All of the comments requested greater flexibility.

Sixteen comment letters sent to FDIC dealt with the proposal implementing Section 315. Many of these commenters stated that the proposal went too far, would be burdensome and expensive, and would hamper timely customer service. Consumer groups objected to the proposal because it did not go far enough with respect to verification and notification.

4. Final Rule

A. Red Flag Regulations.

Identity Theft Prevention Program

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 final regulations provide that 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" (Information Security Standards) issued by the federal banking agencies and the "Standards for Safeguarding Customer Information" issued by the Federal Trade Commission, to implement section 501(b) of the Gramm-Leach-Bliley Act. (The FDIC's Information Security Standards are set forth at 12 C.F.R. Part 364,

Appendix B.) As with the program described in the Information Security Standards, the 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.

Some institutions and creditors may combine their Programs with their information security programs, as these programs are complementary in many ways. As with the Information Security Standards, the FDIC's Red Flag Regulations will apply to state non-member banks and their subsidiaries.

The final regulations list the four basic elements that must be included in the Program of a financial institution or creditor. The Program must contain "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 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 in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

The regulations also enumerate certain steps that financial institutions and creditors must take to administer the Program. These steps include 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 regulations contains detailed guidelines to financial institutions and creditors on how to formulate and maintain a Program that satisfies the requirements of the regulations to detect, prevent, and mitigate identity theft. Each covered financial institution or creditor must consider the guidelines and include in its Program those guidelines that are appropriate. The guidelines provide policies and procedures for use by institutions and creditors to satisfy the requirements of the final rules, including the four elements listed above. While an institution or creditor may determine that particular guidelines are not appropriate to incorporate into its Program, the Program must nonetheless contain reasonable policies and procedures to meet the specific requirements of the final rules. The illustrative examples of Red Flags formerly in Appendix J are now listed in a supplement to the guidelines.

Change of Address Requests for Card Issuers

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 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 provide 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.

In order to provide some flexibility, the final rule clarifies 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.

B. Address Discrepancy Regulations. Section 315 of the FACT Act requires that a nationwide consumer reporting agency (CRA), when providing consumer reports to a requesting user, must 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. Section 315 also requires the Agencies to jointly issue regulations that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy from the CRA.

To implement this provision, the final rules provide that a user must develop and implement reasonable policies and procedures that are 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. These policies and procedures 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 Agencies expect that the user will not use that report.

The final rule provides examples that a user may employ to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. These examples include comparing information provided by the CRA with information that the user (1) obtains and uses to verify the consumer's identity in accordance with the requirements of the CIP rules; (2) maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or (3) obtains from third-party sources. Another example is verifying the information in the consumer report provided by the consumer reporting agency with the consumer.

The final rule also contains a requirement that a user must 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: (1) the user forms a reasonable belief that a consumer report relates to the consumer about whom it requested the report; (2) the user "establishes" a continuing relationship with the consumer; and (3) the user regularly and in the ordinary course of business furnishes information to the CRA. The preamble to the final rule states that a similar requirement for existing accounts exists in Section 623 of the FCRA, which requires users to promptly provide to CRAs complete and accurate information about those accounts.

C. Effective Date. The final rules and guidelines discussed above will be effective the first day of the calendar quarter after publication in the Federal Register. The mandatory compliance date for rules and guidelines will be November 1, 2008.