

10

Satterfield, Kevin

From: Campbell, Vickie [vcampbell@acbankers.org]
Sent: Friday, September 15, 2006 12:38 PM
To: Regs.Comments
Cc: # GOVT RELATIONS; # EXECUTIVE; # COMMUNICATIONS
Subject: America's Community Bankers Comments on Joint Notice-Identity Theft Red Flags Rule, Docket No. 06-07, RIN 1557-AC87
Attachments: Joint Letter-Identify Theft Red Flags 9.15.06.pdf

Attached please find a pdf version of our comment letter regarding the above subject matter.

Steve Kenneally
Director
Payments and Technology Policy
America's Community Bankers
Shaping Our Future
900 19th Street, NW, Suite 400
Washington, DC 20006
202-857-3148 Phone
202-296-8716 Fax
www.americascommunitybankers.org

9/15/2006



September 15, 2006

Office of the Comptroller of the Currency
250 E Street, NW
Mail Stop 1-5
Washington, DC 20219
Docket No. 06-07
RIN 1557-AC87

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 2006-19

Ms. Jennifer Johnson
Secretary
Board of Governors of the Federal Reserve
20th Street and Constitution Avenue, NW
Washington, DC 20551
Docket No. R-1255

Ms. Mary Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
Attention: Comments on ANPR Part 717.
Identity Theft Red Flags

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
RIN 3064-AC04

Office of the Secretary
Federal Trade Commission
Room 159-H (Annex C)
600 Pennsylvania Avenue, NW
Washington, DC 20580
Attention: Red Flags Rule, Project No.
R611019

RE: Joint Notice of Proposed Rulemaking: Identity Theft Red Flags and Address
Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003
July 18, 2006

Dear Sir or Madam:

America's Community Bankers ("ACB") appreciates the opportunity to comment on the Joint Notice of Proposed Rulemaking: Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 ("NPR") issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission (collectively, the "Agencies").

ACB Position

Since December 4, 2003, when the President signed the Fair and Accurate Credit Transaction Act of 2003 ("FACT Act"), ACB has supported its reasonable implementation. ACB is focused on ensuring that the regulatory implementation of the FACT Act provides financial institutions the necessary flexibility to implement appropriate consumer protections without placing an undue burden on our membership.

ACB focuses its comments on the two major areas addressed by this NPR: implementing sections 114 and 315 of the FACT Act. To implement section 114, the NPR proposes requirements for financial institutions to create a written Identity Theft Prevention Program ("Program") to identify patterns, practices, and specific forms of activity that could indicate existence of identity theft. In addition, credit and debit card issuers would be required to establish policies and procedures regarding the validity of address change requests and subsequent requests for replacement or additional cards.

Pursuant to section 315, the NPR proposes that users of consumer reports employ reasonable policies and procedures to detect and mitigate fraud when receiving notices of address discrepancies from consumer reporting agencies.

ACB and its member financial institutions recognize the seriousness of the threat posed by identity theft and related fraud. Identity theft can threaten the fiscal health of a financial institution as well as its reputation. The Identity Theft Red Flags set forth in Appendix J will be of great assistance to financial institutions as they continue to hone their identity theft protection programs.

The regulatory agencies and financial institutions are in agreement on the identity theft threat. Accordingly, the Agencies already have promulgated numerous consumer protection regulations that must be followed by financial institutions.

The Agencies promulgating this NPR recognize the overlapping regulatory requirements imposed in the NPR. In the section describing the estimated burden of complying with the NPR, the Agencies state that most covered entities already have programs to detect and address identity theft as required by Section 114 as a result of customary business practices or because they need to comply with existing regulatory requirements and guidance.

The NPR also requires three separate footnotes (38-40) to list all of the regulations and guidance that it overlaps.¹ ACB believes that these citations represent a large duplication of effort and

¹ The overlapping regulations cited in *Section IV. Regulatory Analysis* by the Agencies in the NPR include the section 326 of the USA PATRIOT Act, the Information Security Standards implementing section 501(b) of the Gramm-Leach-Bliley Act, and section 216 of the FACT Act. The NPR also notes that existing guidance also overlaps the NPR, including Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook's Information Security Booklet, FFIEC's "Authentication in an Internet Banking Environment," and the OCC's "Threats from Fraudulent Bank Web Sites: Risk Mitigation and Response Guidance for Web Site Spoofing Incidents."

require that banks expend resources with only a disproportionately small benefit achieved when completed.

ACB agrees with the NPR that many of the requirements are duplicative, but disagrees with the estimated annual hourly burden required to comply. Even though the information required may be similar, the NPR requires that a formal written report that must cover several specific topic areas be created, reviewed and approved by the Board. The total time estimated by the Agencies to create the Program, prepare the annual report, and train staff is 39 hours annually. This is a very low estimate considering the initial changes in policies and procedures that will be needed to adopt the process and additional reporting format. In addition, the Program will require continual monitoring and updating, increasing the ongoing regulatory burden on financial institutions. ACB members reviewing this proposed rule have provided estimates ranging from 160 hours to 250 hours annually to comply with the requirements.

In light of these concerns, ACB asks that the Agencies review the necessity of standardizing the packaging of the procedures and Program formats and focus instead on the end result of the financial institution's efforts, fraud prevention. The Agencies should review the current rules and regulations that are already in place and rescind this proposed rulemaking and draft an alternative proposal outlining the new requirements in a way that does not overlap with existing requirements.

Our specific concerns about the proposal are outlined below.

SECTION 114

Definitions

The NPR should not expand the definition of consumer reports. Reports used to determine the eligibility of a business, rather than a consumer, for certain purposes, are not consumer reports and the FCRA does not apply to them, even if they contain information on individuals, because Congress did not intend for the FCRA to apply to reports used for commercial purposes. Reports on businesses, or artificial entities, are not consumer reports and the FCRA does not apply to them. That should not change under this NPR.

Section .90 (c) Identity Theft Prevention Program

This section describes the objectives that banks must address in the Program. This section states that the required Program for each bank is flexible based on the size and complexity of the financial institution. However, this statement is accompanied by a long list of mandatory items that must be included in the Program. The list of mandatory items that must be addressed in the Program appears at odds with the emphasis on the "flexible" requirements of the proposed regulation. The items should not be designated mandatory and banks should be allowed flexibility in choosing which items should be addressed by individual banks.

ACB is pleased to note in Footnote 19 Agencies reiterate that the proposed rule should not "unduly burden" smaller institutions with onerous regulations. This is a reference to a

Congressional Record citation attributed to Representative Oxley. We urge the Agencies to strengthen this reference by moving it to the body of the Final Rule and to incorporate this reference into examiner training materials.

Section .90(d) Development and Implementation of Identity Theft Prevention Program

1. Identification and Evaluation of Red Flags

i. Risk Based Red Flags

ACB agrees with the listing of 31 Red Flags identified in Appendix J of the NPR and with the Agencies' understanding that the list is subject to change with individual experience, time and technological advances. This listing is a useful tool for financial institutions to use as a reference when implementing programs to protect their customer accounts.

However, ACB requests clarification regarding updating relevant Red Flag listings. If a financial institution sees the need to add or delete a Red Flag, does the adjustment to the written program need to be approved by the Board of Directors prior to the change being made or can it be noted in the Annual review? Requiring pre-approval by the Board of necessary changes would be counterproductive in the effort to prevent identity theft and impede operations. ACB recommends that any updates to the Program be included in the annual report, but not trigger a need for immediate Board review.

In response to the NPR request for input regarding outside vendors, many financial institutions, especially community banks, rely on third party service providers for core Information Technology ("IT") services, including identity theft, BSA/AML compliance, and SAR reporting. Different IT providers and banks use different techniques and packages to battle fraud and it is difficult to give a specific response to the request in the NPR on how the proposed rule will impact the policies and procedures currently in place, especially with respect to third party providers. Generally, many banks and service providers would need to adjust their procedures, update their policies, and incur additional expenses related to contract changes with third party service providers.

2. Identity Theft Prevention and Mitigation

ii. Verify Identity of Persons Opening Accounts

ACB requests clarification that financial institutions complying with the Customer Identification Program ("CIP") rules required by the USA Patriot Act would be deemed compliant with the NPR requirements. ACB is in favor of this to avoid more overlapping regulations. Although there may be some definitional discrepancies, ACB recommends that a clear statement acknowledging the acceptance of CIP compliance in lieu of the NPR requirements be included in the Final Rule.

iv. Address the Risk of Identity Theft

This section cites actions that financial institutions may take if an account triggers the Program's Red Flag threshold. Included in the list is the option of closing an existing account and denying a new account. However, because a Red Flag threshold was crossed does not definitively demonstrate identity theft is occurring. For example, someone who lost their ATM card last week, may be moving this week, and be robbed next week: none of which mean identity theft has occurred. However, the combination of address changes, new card requests, and fraud alerts could trigger the Red Flag threshold.

ACB is concerned that a financial institution that takes one or more of the actions listed in the proposed section, such as closing existing accounts and denying new accounts, based on the Red Flag thresholds may subject the banks to liabilities if the action taken is later determined to be unwarranted. ACB requests clarification on when closing or denying accounts is required and strongly recommends that a bank be permitted to use its judgment and/or knowledge regarding its customers..

In response to the Agencies' request for comment on whether the measures noted in the section should be cited as examples of actions a financial institution might take, ACB believes that providing examples can be illustrative as long as they are marked as such and do not restrict the actions a financial institution may make, within the confines of the rule.

4. Oversee Service Provider Arrangements

In response to the Agencies' request for comment on allowing third party providers to implement a Program different from its financial institution client, ACB's position is that it should be up to the financial institution client. If a third party provider's Program meets the Program requirements implemented by its client financial institution, it is likely to meet the client's standard. If the third party provider's service level does not meet the requirements of the client, the two entities should negotiate a mutually agreeable solution. The Final Rule should allow this to remain a contractual matter between the two parties.

5. Involve the Board of Directors and Senior Management

ACB concurs that identity theft is an important issue that should be recognized by the Board of Directors in their approval of the Program. It is important to note that the opening of accounts and monitoring for suspicious activity is an operational matter. Because of its operational nature, the development, implementation, and monitoring of the Program is likely to be conducted by bank management and not the Board. The Board should receive an annual report on the Program and any changes that have been made since the previous report. Changes to the Program should not be subject to prior approval of the Board.

The Overview portion of the NPR suggests that financial institutions may integrate the new Program requirements into the Information Security Program that is already required by the Interagency Guidelines Establishing Information Security Standards. The new Program requires Board approval, while an Information Security Program must only be reported to the Board. Accordingly, ACB requests clarification that, if a financial institution chooses to combine the

two Programs, this will not trigger a requirement for Board approval of the Information Security Program.

Proposed Red Flag Guidelines: Appendix J

ACB recommends retaining the provision on inactive accounts in Appendix J. Bankers should have the flexibility to determine when account dormancy is indicative of identity theft. Keeping this provision in Appendix J encourages banks to incorporate this factor into their plans without creating an undue burden.

Section .91 Proposed Special Rules for Card Issuers

The provision that places additional validation requirements on card issuers when replacement cards are issued for accounts with recent address changes would be difficult to implement and require expensive system recoding for financial institutions. The NPR provides an example where additional validations would be required if someone requests a new card within a short time period after changing their address. This would be more easily implemented if address changes and card replacements were the only two activities tracked by the system. However, this requirement would require "time stamps" to be placed on each field within a customer data file and then a logic application would need to be drafted to meet the NPR's requirements. Without making major system changes, financial institutions may have to validate every customer whose data file had been updated or accessed within a determined time period, not just those who updated addresses and then requested replacement cards.

If this section is included in the Final Rule, ACB requests that the Final Rule only apply to "debit" and "credit" cards and that payroll cards and gift cards specifically be exempted.

SECTION 315

Consumer Report User Obligations When Consumer Reporting Agencies Provide Notice of Address Discrepancies

Section .82(c) Requirements to Form a Reasonable Belief

ACB members are subject to the CIP rules used to implement section 326 of the Patriot Act, meeting the standard to form a "reasonable belief" of someone's identity. ACB favors allowing users of consumer reports to use their existing CIP policies and procedures to satisfy the requirements of this proposed section.

Section .82(d)(3) Timing

As the Agencies themselves have recognized, the timing requirements set forth in proposed section .82(d)(3)(i) pertaining to new relationships is problematic. The section essentially requires a user of consumer reports to furnish the consumer's address that it has reasonably confirmed to the consumer reporting agency as part of the information that it regularly furnishes for the reporting period in which it establishes a relationship with the consumer. The practical

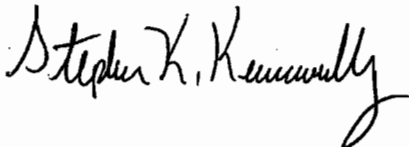
effect of this on those users that choose to use their existing CIP policies and procedures is to require them to establish a reasonable belief that they know the consumer's identity during the same reporting period that they establish a relationship with such consumer. Since a user does not necessarily have control over when a consumer may choose to establish a relationship with it, ACB believes this timing requirement is too stringent and may in some circumstances be impossible for a user to comply with. For example, if a consumer decides to establish a relationship with a user toward the end of a reporting period and the user receives a notice of address discrepancy from the consumer reporting agency within the same period, the user may not have a sufficient enough time left within that period to "form a reasonable belief" that it knows the consumer's identity and provide the consumer reporting agency with the consumer's address that it has reasonably confirmed. ACB believes that a more flexible timing requirement is warranted in connection with newly established relationships. Perhaps the Final Rule should permit users to provide a consumer reporting agency with the consumer's address that it has reasonably confirmed within a reasonable period of time after receiving a notice of address discrepancy from such consumer reporting agency.

Conclusion

ACB appreciates the opportunity to comment on the issue of identity theft and supports the Agencies' efforts to promulgate reasonable rules that will benefit the consumer without placing undue burdens on community banks. The objectives of the NPR are worthy, but many of its requirements are already addressed by pre-existing rules and guidance. For these reasons, ACB recommends that the agencies reconsider this NPR due to the abundance of overlapping regulations and guidance that already apply to banks as they fight identity theft. Any additional regulation should address new issues or areas of concern that are not already covered by existing regulations.

We stand willing to work with the Agencies as the proposed rule is completed. Should you have any questions, please contact the undersigned at 202.857.3148 or via email at skenneally@acbankers.org or Patricia Milon at 202.857.5088 or via email at pmilon@acbankers.org.

Sincerely,

A handwritten signature in black ink that reads "Stephen K. Kenneally". The signature is written in a cursive, flowing style.

Stephen K. Kenneally
Director, Payments and Technology Policy
Regulatory Affairs