citigroup

Carl Howard
General Counsel
Bank Regulatory

Citigroup Inc.
425 Park Avenue
2nd Floor/Zone 2
New York, NY 10022

Tel 212.559.2938
Fax 212.793.4403
howardc@citigroup.com

By electronic delivery

September 18, 2006

Office of the Comptroller of the Currency
250 E. Street, SW.
Public Reference Room, Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 06-07

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

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

Mary F. Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20249

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW.
Washington, DC 20580

Re: Joint proposal of rulemaking to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act")

Ladies and Gentlemen:

Citigroup Inc. "(Citigroup"), on behalf of itself and its subsidiaries, appreciates the opportunity to submit this comment in response to the Joint Notice of Proposed Rulemaking (the "Proposed Rule") regarding identity theft red flags and address discrepancies, published in the Federal Register on July 18, 2006 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") to implement Sections 114 and 315 of the FACT Act.

We commend the Agencies for their collective efforts in this area, although we have a number of suggestions regarding the Proposed Rule as written. We have organized our comments to accord with the specific section of the Proposed Rule to which they apply.

In general, we urge the Agencies to:

1. Clarify that identity theft programs developed by financial institutions should be flexible, risk-based and reliant upon factors which are materially significant in the identification and prevention of identity theft based on the experience, nature and size of the financial institution. They should not be based on a prescribed regulatory checklist of factors which may or may not be relevant to combating identity theft in particular facts and circumstances.

2. Avoid requirements which are not statutorily mandated, such as the application of the Proposed Rules to non-consumer accounts, the application of the address discrepancy requirements to existing customers, and the requirement that a financial institution's Board of Directors approve and oversee that institution's identity theft program.

Subpart I – Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

xx.82 Duties of users regarding address discrepancies

Section 315 of the FACT Act provides that, if a financial institution has requested a consumer report from a consumer reporting agency and that request contains an address which substantially differs from the address in the file of the consumer reporting agency, the agency must notify the requester of the discrepancy. The Agencies are required to prescribe reasonable policies and procedures that a user of a consumer report should employ when the user has received such a notice of discrepancy. Specifically, the FACT Act states that these policies and procedures should enable a user to:

(i) form a reasonable belief that the user knows the identity of the person to whom the report pertains; and

(ii) if the user <u>establishes</u> a continuing relationship…to reconcile the discrepancy by furnishing such address to such consumer reporting agency as part of information regularly furnished by the user…[emphasis added]

Verification of customer's identity. The Proposed Rule states that a user may satisfy the requirement in (i) to verify the customer's identity by following Customer Identification Program ("CIP") procedures pursuant to the USA Patriot Act. The Agencies request comment as to whether those CIP procedures are sufficient. We believe they are.

Verification of address – new customers. With respect to address verification requirements, however, the Proposed Rule becomes confusing. Instead of simply requiring the user to verify the customer's address and supply it to the consumer reporting agency in response to a notice of discrepancy, the Proposed Rule appears to require the user to undertake its verification procedures when it receives the notice of discrepancy. The Supplementary Information confirms this interpretation by stating that a user is required "to take steps to reconcile the address it initially received from the consumer when it receives a notice of address discrepancy..." [emphasis added]

A user typically verifies a customer's address as part of its CIP verification procedures. These procedures may already be complete when it receives notice of an address discrepancy from the agency. The user should be permitted to provide the address, as verified, to the agency instead of having to undergo a reverification process in response to the discrepancy notice.

There appears to be little sense in requiring a user which has already verified a consumer's address to reverify that address after it receives a discrepancy notice. Allowing users to furnish addresses which they have verified just prior to receipt of the notice would satisfy the regulation's objective without imposing a significant, senseless burden on users. Consequently, we request that the language in the final regulation and any accompanying commentary be clarified to permit a user to furnish an address for a new customer which it has already confirmed as accurate for that customer as part of the account approval process.

Verification of address – existing customers. The Proposed Rule would require financial institutions to verify addresses upon receipt of a discrepancy notice even when the customer already has an existing account relationship. This goes beyond the FACT Act, which requires address verifications only when a relationship is "established", as opposed to when an account is "established or maintained", as stated in the Proposed Rules.

There appears to be little added by this requirement. When a customer changes his/her address, the customer typically notifies his/her financial institution, which verifies the new address. The financial institution then reports the new address to the consumer reporting agency as part of the ordinary credit reporting process. Thus, the current system already operates to provide verified addresses to consumer reporting agencies. Requiring financial institutions to verify addresses again at a different point in the reporting cycle would impose a major burden on those institutions with little apparent justification. Consequently, we urge the Agencies to model the final rule on the language which Congress provided and not extend it.

Additional clarifications; business accounts. We request that the Agencies make an additional clarification relating to the applicability of the address discrepancy

requirements. The requirements should not apply where the application for credit has been declined or where the consumer has rescinded the account application. In addition, as stated in greater detail below, the requirements should only apply when the consumer's account is for "personal, family or household purposes", and not to accounts used for business purposes. First, extending these requirements to business accounts goes beyond the reach of the FACT Act, which is a consumer statute. Second, because consumers frequently provide their home address for personal accounts and their business address for business accounts, verifying conflicting addresses would be a very time consuming effort without any apparent benefit in combating true identity theft.

Subpart J - Identity Theft Red Flags

xx.90- Duties regarding the detection, prevention, and mitigation of identity theft.

We urge the Agencies to: (i) modify the coverage of the regulation; (ii) clarify the fact that Identity Theft Prevention Programs should be flexible and truly risk-based, not governed by a set of artificial regulatory criteria; and (iii) reconsider the requirement of Board of Directors approval.

xx.90(b) Definitions

(b)(1) "Account." The Agencies propose a broad definition of "account." We strongly urge the Agencies to limit application to "consumer" accounts for the reasons stated below.

(b)(3) "Customer." The Proposed Rule would require identity theft prevention programs to cover businesses as well as consumers. We urge the Agencies to bring the Proposed Rule in line with the Fair Credit Reporting Act, of which it forms a part, so that it would only apply to consumers who use credit or liability accounts for "personal, family or household purposes."

First, we believe that identity theft per se (as opposed to the broader category of fraud) occurs much more frequently for consumer accounts than for business accounts. Most of the Red Flags have little application to business account fraud, even for fraud related to small businesses.

Second, businesses are in a better position to monitor their own and their employees' activities than are their financial institutions. A business could use the Red Flag guidelines as a means to transfer liability for fraudulent transactions onto its financial institution by alleging, for example, that the financial institution should have detected suspicious activity when monitoring the business's accounts, whereas the business was actually in a better position to do so and to take preventive measures against fraud.

Third, financial institutions already have sufficient incentives to prevent fraud occurring on business accounts without having the additional burden of translating a consumer regulation to the business account environment.

(b)(5) "Red Flags." Instead of defining a Red Flag as "a pattern, practice or activity that indicates the possible risk of identity theft", the universe of possibilities should be narrowed by inclusion of the concept of "materiality" or "significance", based on the knowledge and experience of the financial institution. This would allow a financial institution to make exceptions in cases where the risk of identity theft is lower and to focus compliance efforts where they are most needed.

xx.90(c) Identity Theft Prevention Program

The Agencies should clarify that the regulatory requirement for establishing an appropriate identity theft programs could be satisfied by a flexible risk-based program reasonably designed to detect, prevent and mitigate identity theft, taking into consideration the experience, nature and size of the financial institution. In designing any such program, financial institutions should be permitted to take into account the materiality of any potential risks and the costs, and anticipated effectiveness of potential compliance measures.

"Red Flags" identified in the regulation should be qualified as merely suggestive, and a financial institution should not be required to incorporate a Red Flag in its prevention program simply because that Red Flag could be "possibly indicative" of identity theft. Nor should a financial institution have to prove to examiners the reasonableness of its decision to omit any particular Red Flags in the design of its identity theft program. In addition, under a flexible, risk-based program, financial institutions may legitimately decide to focus less attention on certain types of accounts, such as inactive accounts, low-balance accounts, or accounts sourced by reputable third parties.

Changing identity theft risks. We agree with the Proposed Rule that any identity theft program should be designed to address changing risks over time. The Supplementary Information, however, could be interpreted to require updates every time a new identity theft software program is made available in the marketplace, regardless of other factors, such as the number of previous updates to the program, the magnitude of the anticipated risk, the expense of the new program or its anticipated effectiveness. The Proposed Rule should be modified to require "reasonable periodic" updates rather than "continuing" updates. Since the financial institution is the one who ultimately loses when identity theft occurs, it will have a vested interest in investing reasonable amounts in new programs and technology.

xx.90(d)(1)(ii). Risk Evaluation. The Agencies solicit comment on whether the specified factors are appropriate and whether any additional factors should be considered. We believe that the Agencies should refrain from specifying factors which must be considered by financial institutions, or should at most designate those factors as suggestions or examples. Many different factors could become important in designing or maintaining programs, and these factors could change over time. Since the financial institutions have a vested interest in preventing identity theft, the Agencies should allow them to adopt a flexible approach that considers the likelihood of the occurrence of various types of risk and the potential financial exposure from those risks.

xx.90(d)(3). Staff training. We question why staff training is specifically required under this regulation as opposed to other regulations, absent a specific statutory requirement. We are concerned that this requirement could be read to require standalone training on identity theft, as opposed to training which, preferably, should be integrated into overall staff training on similar or overlapping matters such as fraud prevention.

xx.90(d)(5) Involvement of board of directors and senior management. Again, we question why, absent a specific statutory requirement, board approval is required for identity theft programs, as opposed to other anti-fraud and related management programs. We oppose any requirement that the board of directors or board committee approve a financial institution's identity theft program or receive special annual reports. We believe this requirement could slow down implementation by requiring extensive documentation and could delay any necessary periodic updates. Further, the requirement of board approval could cause unnecessary complications if a financial institution combines the management of identity theft programs with other similar programs to take advantage of synergies and promote efficiency.

xx.91 Duties of card issuers regarding changes of address.

This section implements the specific FACT Act provision that credit and debit card issuers assess the validity of address change requests if they are followed within 30 days by a request for an additional or replacement card. Specifically: xx.91 provides:

> A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account.

Under these circumstances, the card issuer may not issue an additional or replacement card unless the card issuer:

(1) Notifies the cardholder of the request at the cardholder's former address and provides to the cardholder a means of promptly reporting incorrect address changes;

(2) Notifies the cardholder of the request by any other means of communicating that the card issuer and the cardholder have previously agreed to use; or

(3) Uses other means of assessing the validity of the change of address, in accordance with the policies and procedures the card issuer has established pursuant to xx.90. [emphasis added]

We request that the Agencies clarify that a financial institution satisfies its obligations under subsection (3) above if it verifies the address change at the time it is made, whether or not it is subsequently followed by a card request. This procedure ties in with financial institutions' existing procedures which are in fact more protective than the proposal,

since they generally require validation for all address changes, not just those which are followed by requests for new or additional cards. This verification can be done in a number of ways, such as by reconfirming the identity of the consumer requesting the change by use of protected passwords.

We also ask the Agencies to remove the language we have underscored in (3) above, which requires that the "other means" of validating an address change must be pursuant to xx.90. So long as "other means" are effective in assessing the validity of the change in address, they should not be limited to means of validation pursuant to xx.90. For example, it should suffice for purposes of the regulation if a financial institution verifies an address change as part of its general antifraud policies, as opposed to its identity theft policies required by xx.90.

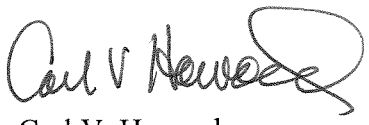
Appendix J. Identity Theft Red Flags.

We have not provided in this letter our comments on the particular Red Flags identified in the Proposed Regulation, since we have provided these comments to various trade organizations for inclusion in their comment letters.

Time required to comply. We urge the Agencies to provide institutions with at least 18 months to comply with the final regulation, since compliance could require systemic and operational changes across many lines of business and could affect interfacing vendors and other third parties that source accounts for institutions.

Again, we thank the Agencies for this opportunity to comment on the Proposed Rule and look forward to working with the Agencies on its implementation. If you have questions on any aspects of this letter, please feel free to call me at (212) 559-2938 or Joyce Elkhateeb at (212) 559-9342.

Sincerely,



Carl V. Howard
General Counsel-Bank Regulatory

cc: Joyce Elkhateeb
Viola Spain