Capital One Financial Corporation
1680 Capital One Drive
McLean, VA 22102

September 18, 2006

Office of the Comptroller of the Currency
250 E Street, S.W.
Public Reference Room, Mail Stop 1-5
Washington, DC 20219
Attn: Docket No. 06-07
regs.comments@occ.treas.gov

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attn: No. 2006-19
regs.comments.ots.treas.gov

Mr. Robert E. Feldman
Executive Secretary
Attn: Comments/
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
RIN 3064-AD00
comments@fdic.gov

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attn: Docket No. R-1255
regs.comments@federalreserve.gov

Ms. Mary F. Rupp
Secretary of the Board
National Credit Union Administration
1775 Duke Street
Alexandria, Virginia 22314-3428
Comments on Proposed Rule 717
Identity Theft Red Flags
regcomments@ncua.gov

Office of the Secretary
Federal Trade Commission
Room 159-H (Annex C)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
Project No. R611019, The Red Flags Rule
https://secure.commentworks.com/ftc-redflags

Re: Interagency Notice of Proposed Rulemaking: *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003*

Ladies and Gentlemen:

Capital One Financial Corporation ("Capital One") is pleased to submit comments on the federal regulatory agencies' (the "Agencies") Notice of Proposed Rulemaking on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit

Transactions Act of 2003 ("FACT Act"), published at 71 Fed. Reg. 40786 (July 18, 2006) ("the Proposed Rule").

Capital One Financial Corporation is a financial holding company whose principal subsidiaries, Capital One Bank, Capital One, F.S.B., Capital One Auto Finance, Inc., and Capital One, N.A. (formerly Hibernia National Bank), offer a broad spectrum of financial products and services to consumers, small businesses, and commercial clients. Capital One's subsidiaries collectively had $47.28 billion in deposits and $108.4 billion in managed loans outstanding as of June 30, 2006, and operated more than 300 retail bank branches. Capital One is a Fortune 500 company, and, through its subsidiaries, is one of the largest issuers of MasterCard and Visa credit cards in the world.[1]

Red Flags Require a Flexible, Risk-Based Approach

In approaching the task of crafting regulatory requirements for financial institutions' identity-theft prevention programs (defining identity theft broadly, as the regulators do, to include account fraud), two facts are worth remembering.

First, financial institutions already have substantial incentives to combat fraud. The motive for fraudsters to attack financial institutions is obvious ("that's where the money is," said Willie Sutton), and in the absence of robust fraud defenses, such attacks would be incessant. Further, in most cases the losses resulting from successful fraud fall on the institution, not on the customer. In the credit card business, for example, the customer's responsibility for unauthorized transactions on his or her account is limited by regulation to $50, and by card-association rule to zero. In consequence, all major financial institutions already possess sophisticated and vigorous anti-fraud programs.

Second, financial services are a complex business, and the systems and procedures necessary to combat fraud both effectively and efficiently are similarly complex, varied, and constantly evolving. Government's prescribing in detail of how institutions should combat fraud would be a mistake, because the prescribed requirements would probably turn out in practice to be cumbersome, expensive, unworkable, ineffective, and obsolete as soon as they were published.

We believe that the Agencies understand these considerations and that, as stated in the Supplementary Information, their intention is to implement the statutory mandates by means of "a flexible risk-based approach similar to the approach used in the 'Interagency Guidelines Establishing Information Security Standards."[2] Capital One commends the Agencies for their determination to take that approach and believes that the framework of the Proposed Rule is largely consistent with that intention.

---

[1] In March, Capital One announced that it has agreed to acquire North Fork Bancorporation, Inc., which operates over 300 bank branches throughout New York, New Jersey, and Connecticut, and is the third-largest depository institution in the greater New York City region. That acquisition, which will make Capital One one of the ten largest banking institutions in the country by deposits, is projected to close by the end of this year.

[2] 71 Fed. Reg. at 40788.

However, the promulgation of a rule with many requirements and a lengthy list of Red Flags (Appendix J) creates a substantial risk that the rule will be enforced in a rigid and formalistic way inconsistent with combating fraud sensibly and effectively. To mitigate that risk, we recommend a small handful of additions to and subtractions from the Proposed Rule.

The following concepts should be added to the language of the Proposed Rule:

- A statement that an institution's identity theft prevention program should be risk-based, focusing on those areas in which the institution's risk assessment shows that the risk of identity theft is significant.

- A statement that the inclusion of a Red Flag on Appendix J creates no presumption that a particular institution must incorporate that Red Flag into its program, if the institution's risk assessment, based on its own business, does not show a significant risk associated with it.

- A statement that an institution may consider the actual incidence of identity theft in comparison with the frequency of a particular Red Flag and the costs or other burdens associated with responding to that Red Flag whenever it appears.

- A statement that the rule does not mandate any specific technology, system, process, or methodology.

Capital One believes that these concepts are probably implicit in the Proposed Rule. However, everyone involved in implementing the rule would benefit if the concepts were made explicit.

We urge that the following concepts be removed from the Proposed Rule as being inconsistent with the practical, risk-based approach that we think the Agencies intend:

- The rule should not define "identity theft" to include *attempts* to commit fraud. Fraudsters will always be attempting to commit fraud ("that's where the money is"). The only way an institution can prevent fraudsters from attempting to commit fraud is to go out of business. A program cannot plausibly be designed to prevent attempts – but that is what proposed section .90(d) would require, when combined with the proposed definition of identity theft. The important thing is not that fraudsters make no attempts at fraud, but that their attempts not *succeed.* Successful identity theft, not unsuccessful attempts to commit it, is the risk the institution's program should be directed against.

- The rule should not define Red Flags to include indicators of "possible risk" of identity theft, rather than "risk" of identity theft or "possible existence" of identity

theft (the latter being the language used in the statute[3]). "Risk" is *itself* "the possibility of suffering harm or loss,"[4] and therefore a "possible risk" of identity theft is the *possibility* of a *possible* loss, a redundancy suggesting a degree of attenuation of risk that, if taken seriously, would require an impossibly cumbersome and overwhelming identity theft program. The Agencies state that their intention in proposing this language is to capture "precursors" of identity theft, such as a security breach or a phishing event; but we submit that, to the extent those precursors raise a significant risk of identity theft, they are fully captured in the concepts of "risk" or "possible existence" of identity theft (and if there can be any doubt on the point, the Supplementary Information and the inclusion of relevant Red Flags on Appendix J would be sufficient to dispel it), and the Agencies should not attempt to capture those precursors by using language suggesting that identity theft programs must spend their effort against attenuated or insignificant risks.[5]

Address Discrepancies

Capital One submits that the FACT Act's address-discrepancy provisions, like the Red Flag provisions, should be implemented in a manner that reasonably enables financial institutions to execute the requirements in the context of their businesses.

Part of that context is that Capital One – probably in common with many other large financial institutions – receives several million address-discrepancy notices from the credit bureaus *every month*. Americans move frequently and sometimes maintain multiple addresses; and in addition, as a general proposition, credit bureaus act as credit bureaus and not as address bureaus. The consumer's address is one item in the bureau's report, but it is not the principal focus of the report (nor is it the main reason the bureau's customers buy the bureau's reports) and it is not normally verified. At one time Capital One conducted an internal survey and concluded that 20 to 30 percent of its requests for bureau reports generated address discrepancies.

Against the background of that enormous volume of discrepancy notices, it is imperative that the statute be implemented in a reasonable and cost-effective way. We commend the Agencies for having taken a critical step in that direction by authorizing

---

[3] Amended FCRA § 615(e)(2)(A).

[4] American Heritage Dictionary of the English Language, 4th edition, p. 1503 (2000).

[5] The Agencies point out that the statute refers, in a different paragraph, to "possible risks to account holders or customers or to the safety and soundness of the institution or customers" (paragraph (1)(B)), but the statutory provision requiring the Agencies to develop guidelines identifying Red Flags (paragraph (2)(A)) uses the more accurate term "possible existence." Congress, not always the most precise congregation of authors, may plausibly have used the term "possible risk" in paragraph (1)(B) to emphasize that the statute was directed at the possibility of identity theft rather than its eventuality in every case; but there is no need for the regulators, whose task is to give language deliberate attention in the rulemaking process, to use that ambiguous terminology in a rule implementing a different paragraph in which even Congress was able to speak with sufficient precision.

institutions to rely on their Customer Identification Programs to satisfy the statute's requirement that the user of the report "form a reasonable belief that the user knows the identity of the person to whom the consumer report pertains." This is a decisively important position for the Agencies to have adopted. We submit that the Agencies should clarify that, if the information user has verified the identity of the customer at account-opening through application of the Customer Identification Program, the fact of its having done so provides the user with a continuing reasonable belief that it knows the identity of the customer in the event that there are subsequent address-discrepancy notices, because the results of the identity check are unlikely to change over the life of the account.

The Agencies' proposed treatment of the statute's other requirement – the address-reconciliation requirement – raises some issues.

The FACT Act provides that if the address discrepancy arises in connection with a newly established account, then the user must "reconcile the address of the consumer with the consumer reporting agency *by furnishing such address to such consumer reporting agency* as part of information regularly furnished by the user …" (emphasis added).

In contrast to the statute's requirement that the user "form a reasonable belief that the user knows the *identity* of the person" (emphasis added), the statute contains no similar requirement that the user form a reasonable belief that it knows the person's correct *address*. However, the Agencies have created such a requirement by proposing that the address the user furnishes to the bureau after receiving a discrepancy notice be "an address … that the user has reasonably confirmed is accurate." Against the background of rampant address discrepancies described above, many of them created by consumers themselves, the additional burden imposed by the Agencies' expansion of the statutory obligation is likely to be enormous, with potentially serious effects on the efficiency of the American lending industry's credit-granting and credit-management functions.

In addition, while the statute's address-reconciliation obligation is activated only if an account is established and requires furnishing a reconciled address only *"for the period in which the relationship is established"* (emphasis added), the Agencies propose that the obligation continue for the duration of the relationship. This aspect of the Proposed Rule, too, greatly expands the burden of the reconciliation obligation; in Capital One's case, not surprisingly, the number of address discrepancies that arise in the course of account management is several times the number that arise upon account origination.

It is very important to avoid potential damage to the efficiency of the credit industry that the Agencies remove these two aspects of the Proposed Rule: the requirement of "reasonable confirmation of accuracy" and the requirement that reconciliation continue for the duration of the customer relationship.

Turning to the specific means of verification proposed in the rule, in light of the industry realities described above the Agencies will appreciate that the first proposed means – verifying the address with the consumer – is unlikely to be feasible on a mass scale. (Even at account origination, when an address discrepancy could be an indicator of possible fraud and hence extra effort would be justified, verifying the address with the applicant would likely generate the same suspect address and hence be of little value. Other means of screening for fraud must be used.) We submit that the Proposed Rule's following two verification provisions – reviewing the user's own records, and verifying the address through third-party sources – should be interpreted as economically as possible. For example:

- An address that matches the lender's past records and that has been submitted to credit bureaus in the past without generating a discrepancy report should be regarded as validly verified.

- An address that, when submitted to a credit bureau (a "third-party source," in the language of the Proposed Rule), has *not* generated a current address discrepancy from that bureau should be regarded as validly verified even if it has generated an address discrepancy from other bureaus.

Duties of Card Issuers Regarding Changes of Address

In implementing the statute's change-of-address provision, too, the Agencies should recognize that the volume of valid address changes and card requests dwarfs the number of fraud attempts. Capital One's card business receives about 10 million address-change requests a year. Of those, about 2 million are followed by requests for additional or replacement cards. Of those 2 million requests, less than *five one-hundreths of one percent* turn out to be fraudulent.

Institutions should be authorized to implement compliance with the statute so that they may cost-effectively process the legitimate requests, serving their customers' real needs, while winnowing out the fraud attempts. There are doubtless many ways to do this. In most cases, given the volumes reported above, it is not cost-effective to contact the customer, so the majority of fraud screens will rely on the statute and Proposed Rule's third, catch-all provision: "other means of assessing the validity of the change of the address." The Agencies should recognize that this will necessarily be so, and that programs that make little use of the cardholder-contact provisions can nevertheless be fully effective and compliant.

For example, it would be plausible for the screening methodology in response to the initial address-change request to be sufficiently effective to validate the address change that it would by itself constitute "other means of assessing the validity of the change of address," even if no special screens were subsequently erected at the card-request stage.

Capital One's procedure is to ask screening questions at the time of the address-change request; then, if the address change is followed by a card request (an indicator of somewhat higher risk), to ask a more extensive and intrusive set of screening questions. Only if that second screen is passed will the card be mailed. Further, depending on the pattern of answers to those second-stage questions, in some cases the card will be mailed but a further review by Capital One's fraud specialists will be conducted while the card is in the mail. If that review indicates a risk of fraud, the card will be deactivated before it arrives.

Capital One submits that this process is sufficient to meet the requirements of the statute and Proposed Rule. In particular, we submit that the additional or replacement card has not been "issued," within the meaning of the statute and Proposed Rule, unless an activated card is delivered. That understanding serves the purpose of the statute – to prevent fraudsters from obtaining a tool with which to commit fraud – while at the same time enabling the card issuer to meet the needs of its many customers who legitimately need their replacement cards, sometimes on an urgent basis so that they may carry on their daily lives.

* * *

Capital One appreciates the opportunity to comment on the Notice of Proposed Rulemaking on Identity Theft Red Flags and Address Discrepancies. If you have any questions about this matter and our comments, please call me at (703) 720-2255.

Sincerely,

/s/

Christopher T. Curtis
Associate General Counsel
Policy Affairs