The Huntington National Bank
Legal Department
Huntington Center
41 South High Street
Columbus, Ohio 43287

September 15, 2006

John C. Dugan
Comptroller of the Currency
Office of the Comptroller of the Currency
250 E Street, SW
Public Reference Room, Mailstop 1-5
Washington, D.C. 20219
regs.comments@occ.treas.gov

Jennifer J. Johnson
Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, D.C. 20551
regs.comments@federalreserve.gov

Attention: OCC Docket No. 06-07; RIN 1557-AC87
Federal Reserve Docket No. R-1255

Re: Notice of Proposed Rulemaking—Red Flag Proposal
71 *Fed. Reg.* 40786 (July 18, 2006)

Dear Mr. Dugan and Ms. Johnson:

This letter is submitted on behalf of The Huntington National Bank ("Huntington")[1] in response to the Notice of Proposed Rulemaking with respect to identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (the

[1] Huntington is a subsidiary of Huntington Bancshares Incorporated, which is a $36 billion regional bank holding company headquartered in Columbus, Ohio. Along with its affiliated companies, Huntington has more than 140 years of serving the financial needs of its customers, and provides innovative retail and commercial financial products and services through more than 375 regional banking offices in Indiana, Kentucky, Michigan, Ohio and West Virginia. Huntington, along with its affiliated companies, also offers retail and commercial financial services online at www.huntington.com; through its technologically advanced, 24-hour telephone bank; and through its network of over 1,000 ATMs. Selected financial service activities are also conducted in other states including: Dealer Sales offices in Arizona, Florida, Georgia, North Carolina, Pennsylvania, South Carolina, and Tennessee; Private Financial and Capital Markets Group offices in Florida; and Mortgage Banking offices in Florida, Maryland and New Jersey. International banking services are made available through the headquarters office in Columbus and an office located in the Cayman Islands and an office located in Hong Kong.

"Notice") published jointly by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the other federal banking agencies and the Federal Trade Commission (collectively, the "Agencies"). We appreciate this opportunity to comment on the Notice.

In general, we appreciate that the Agencies describe these red flag and other requirements several times throughout the Supplementary Information as risk-based and flexible. For example, the written identity theft program must be "based upon the risk assessment of the financial institution" and "must be appropriate to the size and complexity of the financial institution . . . and the nature and scope of its activities, and be flexible to address changing identity theft risks" and the institution may "combine its program to prevent identity theft with its information security program".[2] Furthermore, the Agencies say that the red flag rule was drafted "in a flexible, technologically neutral manner that would not require financial institutions or creditors to acquire expensive new technology to comply".[3] However, notwithstanding the foregoing and other expressions in the Notice that these rules are meant to be risk-based and flexible, what the Agencies are actually proposing is a quite rigid and prescriptive set of specific and onerous requirements that in large measure appear to have lost sight of the ultimate goal of preventing identity theft and reasonable and resource-efficient ways to get there, and instead has become bogged down in inefficient and unnecessary process details. This approach will significantly impair efforts by financial institutions to devote their limited resources to the implementation and development of system-based and other approaches to thwart the real problems and causes of identity theft and prevent fraud.[4]

In general, this red flag identity theft prevention program in the proposal as drafted would appear to require financial institutions to identify every *possible* risk of *attempted* fraud that involves misuse of identification or other account information, address this extensive detail in a written policy that must be approved and periodically reviewed by the institution's board of directors, specifically train all of the institution's employees in the program, and implement the program by capturing every instance of such *possible* risk of *attempted* fraud, evaluating each instance against each of the identified red flags (at least 31 to begin with, and changing frequently) and documenting that evaluation to demonstrate why each and every red flag was or was not an indicator of identity theft in that particular situation. Since every transaction in every account at the institution is fraught with the *possible* risk of *attempted* fraud, this proposal literally appears to be saying that all of that must be done for each and every transaction on each and every account held by the institution.

---

[2] 71 *Fed. Reg.*, at 40788.

[3] 71 *Fed. Reg.*, at 40791.

[4] The Agencies should remember that most instances of fraud that occurs through identity theft—*i.e.*, unauthorized use of an account or forged signatures on checks—result in liability that the financial institution must absorb under the unauthorized use rules in the Truth in Lending Act and Electronic Funds Transfer Act and in provisions of the Uniform Commercial Code allocating risk for forged signatures on checks. Thus, in addition to the incentive provided by the competitive need for exemplary customer service, the institution has every reason to devote substantial efforts to successfully control the risks of identity theft and fraud in order to limit its own financial losses.

For example, the proposed red flag rule says that "[t]he Program must include policies and procedures to identify Red Flags, singly or in combination, that are relevant to detecting a possible risk[5] of identity theft [defined as "a fraud committed or attempted"[6]] . . . using the risk evaluation set forth in paragraph (d)(1)(ii) [pursuant to which the institution "must" consider four named elements] . . . [and] [a]t a minimum, the Program must incorporate any relevant Red Flags from [four listed sources]", presumably meaning that every red flag needs to be evaluated to determine if it is relevant (emphasis added).[7] This proposed provision goes on to say that "[t]he Program must include . . . policies and procedures to . . . [d]etect the Red Flags identified" and to "[a]ssess whether the Red Flags detected . . . evidence a risk of identity theft", going on to say that "[a]n institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft", apparently meaning that even those red flags that do not evidence a risk of identity theft need to be evaluated and documented every time as to why they are not applicable (emphasis added).[8] Even though the proposed rule at that point goes on to say that the institution must then "[a]ddress the risk of identity theft, commensurate with the degree of risk posed, such as by" doing certain enumerated examples, the effort required before getting to this point is literally evaluation, checking off and documenting every red flag for every *possible* risk of *attempted* fraud (and every potential foreshadowing thereof), and all of that regardless of the comfort level the institution has with the identify of the customer or legitimacy of the transaction, not to mention that most transactions will not have any substantial or even likely risk of identity theft or fraud.

Essentially, we believe the Agencies have the process reversed from what it should be. The Agencies are proposing to require this costly and exhaustive process for accounts and transactions whether or not there is any identity theft or actual fraud going on there, instead of allowing the institution to focus attention and resources on where the problems really are, namely, those accounts and transactions where there is or is reasonably likely to be actual fraud or accounts where the identity of the customer is in question or cannot be verified. The Agencies' approach is rather like conducting a search and rescue operation at sea by starting at the North Pole and carefully working south within a detailed grid to track every inch of the world's ocean surface until the lifeboat is found, rather than going first to the place where the lost vessel was last heard from. The former approach may turn up a few seals that no one knew

---

[5] In the Supplementary Information, the Agencies state that they "believe that a 'possible risk' of identity theft may exist even where the 'possible existence' of identity theft is not necessarily indicated" and thus that "it is important to include . . . precursors to identity theft as Red Flags. . . . Therefore, the Agencies have defined 'Red Flags' expansively to include those precursors to identity theft which indicate 'a possible risk' of identity theft". 71 *Fed. Reg.*, at 40790. Thus, apparently what institutions are supposed to be detecting as red flags are not only every *possible* risk of *attempted* fraud, but also every potential foreshadowing of every *possible* risk of *attempted* fraud. Instead of interpreting the statutory term "possible risk" in the direction of flexibility and in the context of a risk-based assessment, the Agencies have instead gone in the opposite direction and interpreted "possible" to mean the possibility of a possibility.

[6] 16 C.F.R. 603.2(a), incorporated in proposed 12 C.F.R. 41.90(b)(4).

[7] Proposed 12 C.F.R. 41.90(d)(1); 71 *Fed. Reg.*, at 40809.

[8] Proposed 12 C.F.R. 41.90(d)(2); 71 *Fed. Reg.*, at 40809-10.

needed rescuing, but the latter approach is more likely to be of any benefit to the survivors in the lifeboat.

We believe the approach adopted by the Interagency Guidelines Establishing Information Security Standards issued by the federal banking agencies under the Gramm-Leach-Bliley Act (the "Information Security Guidelines") is a better model to replicate in establishing a flexible and truly risk-based program for addressing identity theft. The Information Security Guidelines, unlike these red flag rules in the Notice, contemplate that a financial institution will conduct a "big picture" assessment of the applicable risks, taking into account the likelihood and potential damage of reasonably foreseeable threats, and then direct its resources to the particular accounts and circumstances that meet the profile of heightened risk, instead of stretching available resources past the breaking point by requiring review of every possible instance regardless of degree or likelihood of risk or damage. Under an approach similar to that in the Information Security Guidelines, a list of red flags provided by the Agencies would be examples to supplement the institution's own experience in dealing with identity theft and fraud, instead of a mandatory checklist for institutions to tick off or be examined against.

Turning from the general to the more specific, we offer the following comments on particular elements of the proposal in the Notice:

Definition of "account". The Agencies define a "customer" as a person that has an "account" at the financial institution, and "account" is defined as a continuing relationship through which the customer obtains a financial product or service consistent with section 4(k) of the Bank Holding Company Act. The intent is to provide a definition of "account" that is similar to that used in the various privacy regulations of the Agencies issued under the Gramm-Leach-Bliley Act ("GLBA"). While we agree that the GLBA privacy approach is the right set of covered relationships to be covered by the red flag rules, we are concerned that the use of the term "account" in this particular context is problematic since the term "account" is already defined in the Fair Credit Reporting Act (the statute pursuant to which these red flag rules are being issued) as meaning something different. Thus, we recommend that the Agencies use a different term, such as "continuing relationship". Also, we do not believe coverage should be extended to relationships that are not continuing—doing so would be inconsistent with customer identification program requirements under the Patriot Act as well as with the Agencies' own privacy regulations.

Coverage beyond consumers. The proposed definitions of "customer" and "account" extend these proposed red flag rules to commercial, business or nonconsumer accounts. We believe that these rules do not need to extend beyond accounts of individuals established for consumer purposes. Instances of identity theft have not historically been common with business or commercial accounts. Moreover, we are concerned that extending these rules to such accounts will only create opportunities for commercial customers to exonerate their own negligence in managing their business affairs by shifting the blame to the bank for not "discovering" pursuant to these red flag procedures and alerting the business customer about, for

example, embezzlement or other fraudulent transactions by the customer's own bookkeeper. Even if the Agencies do not make this change, there should at least be recognition in the rules that it is appropriate for the institution to devote most of its efforts at compliance to consumer purpose accounts when so warranted pursuant to a risk-based assessment.

Risk evaluation. The proposed red flag rule requires an institution to consider four factors in identifying which red flags are relevant in a given situation: (i) which accounts are subject to a risk of identity theft,[9] (ii) the methods provided to open these accounts,[10] (iii) the methods provided to access these accounts,[11] and (iv) the institution's size, location and customer base.[12] These factors, particularly in the absence of a risk-based set of requirements, generally appear to be irrelevant to any determination of identity theft or actual fraud. Factors that are relevant, for example, are the number and severity of incidents, analysis of the root cause of such incidents, particular combinations or patterns of events and indicators, overall impact and cost of the incidents under review and the institution's experience with what is important and what is not. We recommend that the Agencies stay away from providing lists of factors that institutions must consider, since at best such lists can only be illustrative and will be undergoing a constant process of change and development as institutions adapt to the ever-changing ingenuity of identity thieves and fraudsters.

Inconsistent with Patriot Act. The Agencies acknowledge in the Supplementary Information that the proposed red flag rule requires use of the customer information program ("CIP") procedures applicable under the Patriot Act to verify the identity of any "customer" as defined in the proposal, whereas "the CIP rules [under the Patriot Act] exclude a variety of entities from the definition of 'customer' and exclude a number of products and relationships from the definition of 'account.'"[13] However, section 615(e) of the Fair Credit Reporting Act—the underlying statute for these red flag guidelines and regulations—indicates that such guidelines are not to be inconsistent with the CIP policies and procedures required under the Patriot Act.[14] Thus, it is difficult to understand why the Agencies believe they have the authority to expand the Patriot Act CIP requirements under these red flag rules in the way they have done. This is another reason why the definition of "account" needs to be more limited as indicated above.

---

[9] Of course, if the standard is a potential foreshadowing of a *possible* risk of *attempted* fraud, they all are subject to this risk, making this factor essentially meaningless as a way to determine which red flags are relevant.

[10] Which, if all accounts, is thus all methods of account opening, which again becomes meaningless.

[11] All accounts again, thus all methods of access, thus again meaningless.

[12] Presumably the institution's size, location and customer base is a relative constant in the context of the postulated continuous daily review, and thus requiring this constant to be considered all the time presumably leads to the same conclusion every time, which again, if not meaningless, is at least pointless. Size of the institution is relevant in any cost-benefit analysis in allocation of resources in a risk-based approach to dealing with fraud and identity theft, but is not a factor in determining which red flags the institution determines are relevant to a particular instance of fraud or identity theft.

[13] 71 *Fed. Reg.*, at 40792.

[14] Section 615(e)(3) of the Fair Credit Reporting Act.

Approval and periodic review by the institution's board of directors. The Agencies acknowledge more than once in the Notice the fast-paced nature of the subject matter they are trying to regulate with this proposal—for example, that it may be difficult for them to keep up quickly enough with the rapidly evolving patterns of identity theft in identifying red flags that institutions must consider.[15] Notwithstanding that acknowledgment, the Agencies require an institution's identity theft program under these red flag rules to be formally approved and reviewed at least annually by the institution's board of directors (or a committee thereof), a requirement that has no basis in the underlying statute. Just as with action by the Agencies, board of director review by its very nature (and particularly in a post-Sarbanes-Oxley world of corporate governance) demands extensive documentation, drafting and review that is not designed to keep up with the fast-paced changes and developments inherent with instances of fraud and identity theft. Employees of the institution charged with complying with the institution's identity theft program will understandably be reluctant to take action inconsistent with such a board-approved program (and in fact, are likely to be criticized by examiners for doing so), particularly such a detailed program as this one is required to be, hindering the institution's ability to adapt quickly to changing circumstances. Furthermore, an institution's board of directors, or even a committee thereof, does not typically have the expertise required to develop and review the details of what is necessary to combat fraud and identity theft that will typically be incorporated into this program. Furthermore, requiring an institution's identity theft program to be approved by its board of directors when many other policies and programs are not subject to such a requirement appears to elevate the importance of this program over others that may be equally or more important. Since Congress has not seen fit to require an institution's identity theft program to be review by its board of directors, we recommend that the Agencies abandon this requirement and allow such a program to be adopted and administered by the institution's management that has the specialized expertise to deal with this subject matter.

Equal Credit Opportunity Act. Footnote 23 in the Notice provides an interpretation of the Equal Credit Opportunity Act ("ECOA") that cannot be correct. We question the need and appropriateness of even addressing this topic in the Notice, but if the Agencies believe it needs to be addressed, we respectfully request that the Agencies reconsider the interpretation they have set out. Essentially, the Agencies have stated that denial of a request for credit because of the existence of a fraud alert or active duty alert in the applicant's credit file at a consumer reporting agency would be unlawful discrimination under ECOA because placing such alerts is a right being exercised by the applicant under the Consumer Credit Protection Act. But it simply cannot be the case that treating the applicant in a manner consistent with the applicant's request, and consistent with statutory requirements, is a form of unlawful discrimination. Section 605A(h)(1)(B)(i) of the Fair Credit Reporting Act ("FCRA") prohibits a user of the consumer report from granting credit "unless the user utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request."[16] In other words, if the creditor wants to extend credit in the presence of a fraud alert or active duty alert in the consumer's credit report, the creditor must take the specified steps to confirm the identity of

[15] 71 *Fed. Reg.*, at 40791.
[16] 15 U.S.C. 1681c-1.

the applicant, but otherwise, the creditor is flatly prohibited from granting credit. The Agencies in footnote 23 have turned this statutory requirement around to make it say that whenever a credit file contains a fraud alert or active duty alert, the creditor "must take reasonable steps to verify the identity of the individual in accordance with the requirements of [this provision of FCRA]." Clearly, that statute does not say that, and thus this footnote should be withdrawn.

Address discrepancies. The Agencies' proposed rules with respect to verification and reconciliation of address discrepancies received from consumer reporting agencies has the potential, if not modified and placed in a risk-based context, to be the most burdensome requirement for unnecessary and useless efforts in all of the Notice. Anywhere from a quarter to a third of an institution's customer base is likely to have an address change over the course of a year—either a new address or an additional or supplemental address (such as a vacation address or a snowbird address)—and it is our experience that virtually all address changes are legitimate and do not indicate fraud or identity theft. Yet this rule requires virtually every notice of an address discrepancy received from a consumer reporting agency to trigger a series of actions on the part of the receiving institution notwithstanding the fact that nothing whatsoever is amiss with the customer's account or transactions. We understand that there is a statutory requirement here that needs to be implemented, but in several ways the Agencies have gone beyond what is required by the statute and unnecessarily increased the resulting regulatory burden in a context when in virtually every instance there is nothing substantial to be gained by the consumer or anyone else because of the low instance of fraudulent address changes. We appreciate that the Agencies have indicated that in meeting the statutory requirement to form a reasonable belief that the user knows the identity of the person to whom the consumer report relates, the institution may rely on the institution's CIP under the Patriot Act. However, in the Supplementary Information the Agencies go on to state that "a user could use its existing CIP policies and procedures to satisfy this requirement, so long as it applies them in all situations where it receives a notice of address discrepancy."[17] It is not clear why use of an institution's CIP procedures would be compliant if used in every circumstance, but not compliant if not used in all circumstances, and this comment should be withdrawn. Additionally, the underlying statute requires an institution to reconcile an address discrepancy with a consumer reporting agency only in the context of the user establishing a relationship with the consumer, but the proposed rule expands this requirement to reconcile the address when the notice of address discrepancy is received with respect to a consumer with whom the institution already has an existing relationship. There is no reasonable basis in this case for the Agencies to issue a rule which exceeds the underlying statutory obligation when in virtually every case the address discrepancy is no indication of any problem. Moreover, the proposed rule requires users to "reasonably confirm that an address is accurate" before reconciling that address by sending it to the consumer reporting agency. There is nothing in the statute that requires this additional step of confirming the accuracy of the consumer's address. In addition to being beyond the statutory obligation, such a confirmation or verification requirement is unnecessary and exceedingly burdensome in a context where virtually every address change is legitimate and where the institution has no

[17] 71 *Fed. Reg.*, at 40795.

reason otherwise to question the consumer's identity. Such a verification requirement will entail substantial additional costs of preparing and mailing out confirmations or otherwise performing reviews of information the institution already believes is accurate, particularly when the institution has probably just obtained such address information from the consumer in the context of the application for the relationship being established. The Agencies should consider that the address furnished by the institution that triggers the notice of address discrepancy from the consumer reporting agency is generally furnished in the context of a request for a consumer report at generally the same time as the institution is reasonably concluding that it knows the identity of the consumer through application of the institution's CIP procedures. Unless there is some other indication that something is amiss, the receipt of a notice of address discrepancy by itself is such a low indicator of a potential problem that triggering all of these additional obligations beyond what the underlying statute requires is unnecessary regulatory burden that the Agencies should abandon.

Effective date. We believe it could take up to 18 months to two years for institutions to be able to come into compliance with these proposed rules, considering their complexity and burden,[18] and considering many of the other statutory and regulatory requirements that financial institutions are also being required to implement at this time, such as compliance with the interagency authentication guidance, do-not-fax rules, SPAM rules, and changes in anti-money laundering, Bank Secrecy Act and anti-terrorist requirements, not to mention initiatives that the institution may be making for its own business or customer service reasons.

Thank you for consideration of these comments. If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me at 614-480-5760.

Sincerely,

Daniel W. Morton
Senior Vice President & Senior Counsel

[18] The Agencies' estimate of the burden associated with this proposal in the Paperwork Reduction Act section of the Notice cannot be a realistic estimate, even as an average. Huntington, for example, has already spent significantly more than 39 person-hours just in reviewing and responding to this Notice, considering that most areas of the institution are affected by this proposal.