1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Nessa Feddis
Senior Federal Counsel
Phone: 202-663-5433
Nfeddis@aba.com

By electronic delivery

14 September 2006

Office of the Comptroller of the Currency
250 E Street, SW.
Public Reference Room, Mail Stop 1–5
Washington, DC 20219
regs.comments@occ.treas.gov

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

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

Mary F. Rupp,
Secretary of the Board
National Credit Union Administration
1775 Duke Street, Alexandria, Virginia 22314–3428
regcomments@ncua.gov

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW.
Washington, DC 20429
Comments@FDIC.gov

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

Re: Joint proposal rulemaking
Implementation of Sections 114 and 315 of the FACT Act
Identity Theft Red Flag guidelines
OCC Docket No. 06-07; FRB Docket No. R-1255; FDIC RIN 3064-AD00; OTS No. 2006-19; NCUA (No Docket Number); FTC RIN 3084-AA94
71 *Federal Register* 40786, 18 July 2006

Ladies and Gentlemen:

The American Bankers Association ("ABA") respectfully submits its comments to the Office of the Comptroller of the Currency, the Federal

Reserve Board, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission ("the Agencies") on their proposed regulations related to implementation of Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"). As required by Section 114, the Agencies are jointly proposing guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. In addition, the proposal includes a provision requiring credit and debit card issuers to assess the validity of a request of a change of address under certain circumstances and a provision related to procedures users of consumer reports must employ when they receive a notice of address discrepancy from a consumer reporting agency.

The ABA on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership--which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks--makes ABA the largest banking trade association in the country.

Summary of Comments.

The ABA and its members have a long history of combating identity theft and financial fraud. Indeed, financial institutions have strong incentives to prevent such fraud: they generally suffer the financial losses and risk customer and public dissatisfaction. This extensive experience and exposure has shown that financial institutions must have broad flexibility to develop and implement appropriate controls to respond effectively to evolving financial crime threats faced by our banks. While the Agencies state that the proposed Regulation is intended to be flexible and reflect a risk-based approach, we conclude that the proposed regulatory language in many cases falls short of these stated intentions. Instead, we believe that the proposal runs a high risk of creating an artificial, stagnant, mandatory checklist regime that will not effectively advance the goals of detecting and preventing identity theft and fraud. We fear that unless these shortcomings are addressed, the result will be a diversion of resources from effective detection, investigation, and corrective action and will necessitate wasteful expenditure on burdensome, paperwork-laden compliance exercises. Bankers' attention will be drawn into wasteful but obligatory drills to justify each judgment call made under a good faith effort to defeat identity thieves and fraudsters.

For these reasons, we strongly recommend that the Agencies substantially simplify the final Regulation and re-cast it to meet the following principles to apply necessary flexibility in the common effort to fight identity theft and fraud:

- Regulate by objective, *not* prescription,
- Take advantage of synergies with existing regulatory standards and operational efficiencies,
- Avoid requirements not mandated by the statute,
- Keep compliance simple, and
- Recognize that *risk-based* considerations work best as guidance and allow for appropriate judgment, rather than rely on fixed rules.

ABA submits its comment in three parts: this letter presenting our salient policy points and concerns about the regulatory framework as proposed, and two attachments—the first detailing our specific criticisms and suggestions about the Regulation, and the second, detailing our criticisms and suggestions about the specific Red Flags set forth in Appendix J.

Regulate by objective, not prescription.

Flexibility to combat identity theft is critical because of the changing nature of fraud practices. Fraud and fraudsters are dynamic, constantly altering methods and targets, as must be the fraud detection techniques and solutions. Fraudsters are continually seeking to detect any vulnerability to exploit: when they encounter an obstacle, they search for a way around it. At one time, the queen's seal and a bit of wax was an effective identity theft tool; today, it is not. We know that any single fraud prevention solution is in danger of becoming obsolete.

Similarly, we can expect the proposed Red Flags to become less effective with time. Like water, the crooks will try to find a way around obstacles once they are identified. The mere notoriety of a red flag is a major step towards its obsolescence as a reliable detector. Yet, under proposed Section __90(d)(2)(iii), financial institutions "must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft. . ." Any financial institution that chooses not to adopt one of the Red Flags from this list does so at its own peril. By insisting on this static, one-size-fits-all-or-tell-us-why standard, the proposed rule converts the Red Flags into a regulatory checklist of mandates regardless of their current effectiveness as fraud detectors.

We believe that this approach misses the purpose of the statutory Red Flag provision, which was to merge the strengths of regulators and financial firms to fight fraud more effectively. The regulators, as gatherers of industry-wide information on fraud experiences, were to share that information with financial institutions to inform the anti-fraud efforts of banks and other financial firms. Industry would use that information to keep design effective, up-to-date anti-fraud programs and keep them current. Instead, the proposal is a look behind approach that is more of an

effort by the regulators to do what the financial industry can do best, namely design and maintain effective anti-fraud programs.

The proposed regulatory approach appears to be at odds with the Agencies' assertion in the Supplementary Information that they "are proposing Red Flag regulations that adopt a flexible risk-based approach similar to the approach used in the 'Interagency Guidelines Establishing Information Security Standards…. Like the program described in the Agencies' Information Security Standards, the [Identity Theft Prevention] Program 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 as they arise***." (Emphasis added.) We support that goal as presented in that description, and we believe that the proposal should be revised to be consistent with it.

Unlike the prescriptive language in the Red Flag Regulation, the Agencies' Information Security Standards present a more flexible, workable approach. The guidelines to that standard, the "Interagency Guidelines Establishing the Standards for Safeguarding Customer Information," set forth instead general objectives to "ensure the security and confidentiality of customer information," "protect against any anticipated threats or hazards," and "protect against unauthorized access." Equally, the Guidelines' directives are focused on key desiderata: "identify reasonably foreseeable internal and external threats that could result in unauthorized disclosures, misuse. . . of customer information. . .," "assess the likelihood and potential damage of these threats. . ." The Guidelines require financial institutions to consider suggested measures, but only those the "the bank holding company concludes are appropriate."

We recommend that the Agencies adopt similar language in the Red Flag Regulation that will allow financial institutions the discretion and flexibility necessary to have up-to-date effective programs that best fit the needs of their customers and their activities. As the Supplementary Information succinctly states, "Ultimately, a financial institution or creditor is responsible for implementing a Program that is designed to effectively detect, prevent and mitigate identity theft." This fundamental objective may be most effectively pursued by describing the regulatory duty to establish an Identity Theft Prevention Program by the simple directive paraphrased from the Bank Secrecy Act, of "developing and providing a program reasonably designed to detect, prevent and mitigate identity theft." Other recommendations toward this goal of effective, flexible, principles-based regulation are suggested in Attachment A.

Take advantage of existing synergies.

The proposed regulation pursues the goal of taking advantage of synergies with existing regulatory standards and operating efficiencies in two noticeable ways that ABA applauds.

First, the Supplementary Information suggests that a financial institution may wish to combine its program to prevent identity theft with its information security program, "as these programs are complementary in many ways."

Second, the proposed regulation implements the statutory directive of conforming to the existing Customer Identification Program (CIP) requirements by stating that banks in compliance with the CIP rules satisfy the proposed Regulation's requirement "to obtain identifying information about, and verify the identity of, a person opening an account."

ABA supports both of these policy positions and encourages the Agencies to recognize that financial institutions have other existing fraud prevention, suspicious activity detection, and security risk management practices and procedures that play a valuable role in detecting, preventing, and mitigating identity theft. To realize the synergies of these existing efforts, the Agencies and their examiners should not expect the Identity Theft Program to be represented as a written document separate and apart from a financial institution's overall financial crime risk management processes as long as such over-arching programs contain the elements appropriate for detecting, preventing and mitigating identity theft.

***Avoid requirements not mandated by the statute*.**

ABA believes that the proposed regulation unnecessarily insists on requirements not mandated by statute. These requirements limit flexibility, impose undue costs, and get in the way of effective identity theft and fraud prevention.

Among the non-mandated regulatory requirements are the following:

- Overreaching scope of Regulation's application
- A written Identity Theft Prevention Program
- A specified obligation for boards of directors that is inequitable

First, since the task at hand is to implement part of the FACT Act, ABA considers the proper scope of the proposed Regulation to be limited to consumer financial services, not business financial services. The statute does not need a definition of "account" to give effect to its terms, let alone a definition that expands coverage to business purpose credit or services.

Second, while the statute calls for reasonable procedures for implementing Red Flag guidelines, it does not demand the formality imposed by requiring a written Identity Theft Prevention Program. As previously noted, identity theft prevention is an initiative seamlessly integrated in institutions' financial fraud and crime risk management

processes. Carving out a separate writing for a capital “I”, capital “T”, capital double “P” –Identity Theft Prevention Program—exalts form over the very real substance of efficient, broad-based fraud deterrence systems and will only lead to examiners and auditors insisting on dotted “I”s , crossed “T”s, and well-rounded “P”s.

Third, no whisper of board involvement is mentioned in the law, yet the proposed Regulation creates a novel definition of board of directors that ends up imposing a management duty on boards of directors for financial institutions (yet leaves this responsibility to the lowly “designated employee” in companies lacking formal boards). Further, blurring of responsibilities between management and board was wisely not mandated by Congress and is a distraction from the important goal of fighting identity theft.

In addition, flexibility may be further reduced by the requirement that the board of directors approve the program. By nature, programs requiring board approval demand extensive documentation and very deliberate drafting as well as very particular administrative review. Yet, also by nature, fraud and identity theft pop up quickly and demand a nimble, quick, and sometimes discrete response. Management may be reluctant to respond by taking an action not yet contained in the official, board-approved Program, especially if it is different from the current Program. Requiring board approval of a Program hinders change, which is critical when addressing fraud. Boards do not shoulder such detailed approval obligations for fraud systems today, and no case has been presented demonstrating the need to involve boards in the details of any one specific class of fraud threat.

Notably, in the Supplementary Information the Agencies excuse their own inability to coordinate their respective formal regulatory structures to meet the statutory mandate to update the Red Flags “as often as necessary” or “quickly enough to keep pace with rapidly evolving patterns of identity theft,” but then would impose a non-statutory requirement for more administrative procedure on banks. (See e.g., 71 Federal Register at 40791, text and footnote 20.)

ABA believes these invented requirements and other non-mandated aspects of the proposed Regulation discussed in Attachment A are unnecessary and in fact harmful to effective programs to address identity theft.

Keep compliance simple.

As proposed, the Regulation erects a number of burdensome compliance exercises that limit flexibility and add costs, which in turn sap resources from the ultimate objective of combating identity theft. In addition to the non-mandatory elements of the proposed Regulation, the

rigidity of the Red Flag implementation process is also riddled with unnecessary compliance hurdles.

For example, under proposed Section __90(d)(1), "At a minimum, the Program must incorporate any relevant Red Flags" from the proposed Appendix J as well as from other sources, including supervisory guidance, incidents of identity theft the financial institution has experienced, and new methods of identity theft the financial institution has identified. While the proposal qualifies this requirement with "relevant" Red Flags, the provision in effect imposes a mandatory review, analysis, and report of the Red Flags proposed in Appendix J and elsewhere, and of virtually any new identity theft incident or trend and potential fraud prevention measure, regardless of likely continuation, application, or impact on the financial institution or its customers. And these reviews, analysis, and reports are continuing.

Similarly, under proposed Section __90(d)(1)(ii), financial institutions "must consider" certain factors in identifying whether particular Red Flags are relevant. Many institutions may, in fact, consider these factors, but they may be indirectly factored into an overall design or categorized differently, for example. Some with effective identity theft and fraud prevention programs may not use these factors at all while relying on others just as—or even more—relevant or reliable. As a compilation in an official regulation, however, they achieve a priority status, becoming an artificial checklist for the financial institutions ***and their examiners***, requiring financial institutions to reconstitute their approach to the Identity Theft Program, when doing so does not advance the goals of the Program. Identity Theft Programs are thereby drawn to a uniform average that the Agencies themselves admit that they themselves cannot keep current and up to date. Identity Theft Programs in practice become hobbled by a backward looking ball and chain, when, ironically, the provision in the law was enacted to direct the Agencies to provide the information that financial institutions could use to keep their Identity Theft Programs forward looking and ahead of the crooks. Under the proposal, too much attention by financial institutions will be directed toward regulators in a distracting compliance exercise.

The proposal assumes that all the Red Flags are relevant to every financial institution and puts the burden on the financial institution to research, analyze, document, and then persuade examiners that a particular Red Flag does not apply to a product. In many cases, it will be self-evident that a Red Flag does not apply, but the financial institution will nevertheless have to justify and document its exclusion. This is contrary to Congressional intent, which was that Red Flags be an aid to industry, not a nuisance.

Moreover, financial institutions will have to incur costs to re-design identity theft and fraud programs into artificial packages in order to fit into

the regulatory scheme examiners will expect. In practice, many identity theft and fraud prevention components are integrated throughout the institution, from the teller to the back office, and not neatly set out to conform to the proposed regulatory list. To ensure that financial institutions retain the ability to design the most effective solutions, which they have a substantial incentive to do, since they usually suffer on average a $10 loss for every $1 lost by their customers—added to which is very understandable customer dissatisfaction—it is critical that they have broad discretion in designing their Programs and that they not be expected to navigate an arbitrary checklist with their examiners.

As prescriptive as the proposed regulation is, it invites examiner and internal auditor micro-managing and potentially pointless criticism—not because a bank's program does not detect or prevent identity theft, but because it does not have all the required regulatory paperwork justifying each and every element either contained or not contained in the Program.

The regulations should emphasize risk-based consideration.

ABA endorses true risk-based compliance. There is wide latitude in such an approach for banks to conduct their business. ABA believes that risk-based judgments by banks about their identity theft practices and procedures should receive deference by the Agencies, not just lip-service.

The key to any risk-based approach is the ability to evaluate the likelihood and severity of adverse events and to prioritize one's response in a manner that applies greater resources to the event of greater expected significance and fewer resources to events of lesser significance. In other words, control programs are to be tailored to expected experience.

Too often of late, "risk-based" has become a label for a supervisory expectation that banks must identify all the risks and build elaborate controls, with equally elaborately documented evaluations, for every one of them. A genuine risk-based approach should lead to prioritizing the importance of various controls, addressing the most important risks first and accepting the good faith judgments of banks in differentiating among their options for conducting safe, sound and compliant operations.

How financial institutions go about a risk-based approach varies widely, as do the risks themselves and the environments in which they occur, and can be just as successful informally in modest risk circumstances as when formally conducted in diverse, complex operations. Accordingly, the regulation itself should stress the risk-based aspect of Red Flag Programs.

In addition, ABA is concerned that institutionalizing detailed Red Flags and fraud mitigation measures will hasten the obsolescence of

those factors as they become the opening chapter for *Fraudsters for Dummies* or *The 31 Habits of Highly Effective Identity Thieves.* For example, the proposal suggests flagging purchases made at jewelry or electronic stores. Fraudsters will know to make those purchases at department stores, where the type of merchandise involved is unknown to the issuer. Listing such details of specific fraud prevention measures in a public regulation merely shortens the life of that solution. Accordingly, we encourage the Agencies to avoid where possible unnecessary public dissemination of specific details. We provide in Attachment B specific suggestions in our comments on the particular Red Flags of the proposed Appendix.

The Agencies should adopt an Official Staff Commentary.

In keeping with the goal of providing assistance to industry risk-based judgment, we also strongly recommend that an Official Staff Commentary accompany the final Regulation, as is the case with many other regulations. We believe that a Commentary will be critical to financial institutions for implementation of the Regulation as well as for continued compliance. A Commentary will ensure that financial institutions have convenient access, in an understandable format, to important guidance related to the final Regulation. Further, the Agencies will have a mechanism for providing additional guidance as the need arises.

Conclusion.

ABA and its members have been in the forefront of fighting identity theft. Furthermore, we have continued to adapt ourselves and our tools to this fight in the 20 months since the FACT Act was passed and will continue to detect, deter, and defend our customers and our financial institutions from these threats going forward with or without regulatory intervention.

ABA firmly believes that the creativity, ingenuity, and agility required to respond to those who would perpetrate identity theft and financial fraud can only succeed in an objective-based, non-prescriptive regulatory environment that recognizes existing operational synergies, avoids unnecessary non-statutory mandates, keeps compliance simple, and emphasizes deference to risk-based bank judgments expressed in flexible guidance, rather than rigid regulation.

Consequently, we strongly advocate simplifying the Regulation and revamping the Red Flag guidelines to put the emphasis where it belongs—on reasonably designed procedures that assist banks in fighting identity theft prevention, rather than on new regulatory programs with reams of identity theft compliance documentation that divert resources from the problems we all wish to solve.

We appreciate the opportunity to provide our comments to this important proposal and are pleased to provide any additional information.

Sincerely,

Nessa Eileen Feddis

Attachment A

Specific Comments

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

__82 Duties of users regarding address discrepancies.

Section 315 of the FACT Act requires that when providing consumer reports to requesting users, nationwide consumer reporting agencies must provide a notice 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. In addition, FACT Act requires the Agencies to jointly issue regulations providing guidance regarding reasonable policies and procedures that users of a consumer report should employ when the user has received a notice of discrepancy. The regulations must describe reasonable policies and procedures for users of the report to:

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

(2) reconcile the address of the consumer with the consumer reporting agency by furnishing such address to the consumer reporting agency as part of the information regularly furnished by the user for the period in which the relationship is established if the user establishes a continuing relationship with the consumer.

(b) Definition.

The proposal defines a "notice of discrepancy" as:

> [A] notice sent to a user of a consumer report by a consumer reporting agency that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

We agree with this proposed definition because it limits the requirement to occasions where there is a "substantial" difference between the addresses. Discrepancies due to, for example, "fat fingers" or inverted numbers, should not trigger the provision, which the Supplementary Information should acknowledge.

(c) Requirement to form a reasonable belief.

Pursuant to the statute, this proposed provision requires users to develop and implement reasonable policies and procedures for verifying the identity of the consumer for whom it has obtained a consumer report and received a notice of address discrepancy. It specifically provides that a user who develops its CIP, based on the requirements of section 326 of the USA PATRIOT Act satisfies this requirement. We agree that it is sufficient for users to verify the "identity" of consumer based on CIP requirements. We therefore support the proposed provision which provides that use of CIP procedures is adequate. This helps to avoid unnecessary duplicative requirements

We suggest, however, that the Agencies clarify that users receiving a notice of discrepancy are not required to re-verify the identity of the consumer upon receipt of a discrepancy if they have already completed their customer identification pursuant to CIP. The proposed language requiring a user to develop and implement reasonable policies and procedures for "verifying the identity of the consumer for whom it has obtained a consumer report and for whom it receives a notice of address discrepancy" could be interpreted to mean that if the user receives the notice of discrepancy after completing CIP, it must re-verify the identity of the consumer. We believe this would be unnecessary and duplicative.

(d) Consumer's address

(1) Requirement to furnish consumer's address to a consumer reporting agency.

(2) Requirement to confirm consumer's address.

Under this provision, users must develop and implement reasonable policies and procedures for "furnishing an address for the consumer that the user has reasonably confirmed is accurate," when the user

- can form a "reasonable belief that it knows the identity of the consumer";
- establishes or maintains a continuing relationship with the consumer; and
- regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy was obtained.

Users may reasonably confirm the address is accurate by:

(1) Verifying the address with the person to whom the consumer report pertains;

(2) Reviewing its own records of the address provided to request the consumer report;

(3) Verifying the address through third-party sources;

(4) Using other reasonable means.

Our concern with these proposed provisions is that they may add new burdens to verify the address when doing so will not improve accuracy or prevent identity theft beyond what current practices do. However, it will add costs and delays as well as frustrate and inconvenience consumers. We believe that complying with CIP rules to verify the "identity" of the consumer is sufficient and better reflects Congressional intent. Accordingly, we strongly recommend that the final regulation either eliminate the requirement to verify the address or provide that customer identification validation processes completed pursuant to CIP requirements of section 326 of the USA PATRIOT Act are sufficient to satisfy the address verification requirements provided for this in this Regulation.

The fact is, people move all the time and often use multiple addresses for a variety of perfectly valid reasons. Large financial institutions report that they receive thousands of legitimate change of address notices each day. Usually, consumers do not notify the consumer reporting agency of this move or additional address. Instead, consumer reporting agencies use other efficient and reliable means to update reports with new addresses. When a financial institution user receives a consumer report with an address different from the one the applicant provided, it confirms the applicant's identity consistent with CIP rules. If the account is opened, the financial institution user submits the new address in the course of its regular account reporting to the consumer reporting agency. Assuming the user is a reliable source, the consumer reporting agency then confirms the information through its established internal procedures prior to adding this new address to the report. In the event an existing customer changes a billing address, this new address is provided to the consumer reporting agency in the usual course of reporting to the consumer reporting agency. This current system is a very effective and efficient way to update addresses in consumer reports.

The extra precautions provided for in this proposal to verify the address are unfounded, as these validation procedures are well documented in the account opening CIP procedures established by each financial institution. Merely confirming the existence of these policies and procedures in adherence to existing requirements of the USA PATRIOT Act will ensure that the essence of this proposal is reiterated through existing regulatory requirements. We recommend that this proposed provision either be deleted to avoid duplication through existing regulatory

requirements or be amended to refer to them. Duplication of policies and procedures to adhere to differing regulatory requirements can be futile and cause additional, unwarranted burdens on financial institutions.

We also object to expanding the statutory requirement to apply to instances where an account is not being established, but already exists. Financial institutions pull consumer reports on existing customers for a variety of reasons, among them, to review the customer's continued eligibility for the product and terms. While the institution itself may receive a report that includes the address, often, particularly among large institutions with high account volumes, the institution filters information other than the credit score. One reason for this policy is to protect consumer report information and minimize who has access to it. In these cases, if a notice of address discrepancy is on the report, that notice will not reach the department reviewing the account. Financial institutions will be forced to obtain and relay the entire report and implement new processes to respond.

This additional burden is not necessary because the current system already has a mechanism for updating addresses for existing customers. Furnishers currently report new address information obtained from the customer when they provide account updates in the usual course of reporting. Moreover, we believe that Congress recognized that it was not necessary and clearly and deliberately intended to minimize additional regulatory burden by limiting requirement to instances where an account is "established."

Subpart J – Identity Theft Red Flags

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

(**b) Definitions**

(1) Account. The Agencies are proposing a broad definition of "account" to include not only consumer accounts, but also business accounts. We strongly urge the Agencies to limit application to consumer accounts. (See comments to definition of "customer.")

The Agencies request comment on whether the definition of account should also include relationships that are not "continuing." We strongly urge not expanding the definition. Defining an area with such a broad brush will cause a burden on financial institutions to gather and maintain information on non-customers for single transactions performed. In general, financial institutions have limited interactions with non-customers. In some situations this may include the sale of a money order or issuance of a low dollar wire transfer. Although information is retained

pertaining to the transactions, credit reports are not necessarily warranted to validate information provided.

(3) Customer

The proposal defines “customer” broadly, to include not only individuals, but also businesses. We strongly urge the Agencies to exclude business customers from the definition. One reason to exclude business accounts is that most of the proposed Red Flags have little if any application to business account fraud, even for fraud related to small business accounts. For example, many of the Red Flags are related to information contained in consumer reports, including addresses, that commonly are not used or relevant to a business account. Consumer reports might be used to determine creditworthiness of principals, but not to verify the identity and address of the business. Nevertheless, financial institutions would have to analyze, document, and review periodically the reasons each of the Red Flags is not relevant in the business context.

Furthermore, while business identity theft may and does occur, it is far rarer for a number of reasons. Banks perform different due diligence when opening a business account for reasons beyond just identity theft: they have to ensure the viability of the business and rely on information other than a consumer report. In many instances, corporation documents and resolutions are provided to ensure that the account signatories have the appropriate authorization to enter into a contractual agreement to conduct financial transactions on behalf of the business. Moreover, businesses, which are presumed to be more sophisticated than consumers, are in a better position to protect themselves against fraud than consumers, both in terms of prevention and in enforcing their legal rights.

We are also concerned that, if experience is a guide, businesses will use the Red Flags as a means to shift responsibility from themselves to the banks, even though the businesses may be in a better position to prevent fraud. This is especially true, given that the broad definition of “identity theft” includes potentially any fraudulent transaction on any existing financial account. For example, businesses could use the regulation and guidelines as a basis to assert that the bank should have detected fraudulent transactions by a dishonest bookkeeper on the basis that the transaction was an “unusual” transaction. Such an approach moves toward absolving businesses from performing due diligence in hiring employees and monitoring accounts. Already, banks report that businesses are using Suspicious Activity Report requirements in attempts to shift liability and responsibility to banks. We do not believe that the Red Flag guidelines were intended or should be used to relieve businesses of their current responsibilities related to fraud prevention and detection.

Including businesses is also inconsistent with the Interagency Guidelines for Safeguarding Customer Information, which limits "customers" to consumers. To the degree that the requirements of the proposal and the Guidelines for Safeguarding Customer Information dovetail, as the Agencies suggest that they do, in the interest of minimizing compliance complexity and burdens, we believe that the definitions should be consistent. Otherwise, it becomes more complicated to marry the two regulations in a compliance environment.

In any case, financial institutions already have sufficient incentives to prevent business identity and do not ignore their business customer vulnerability. That there is a fraud risk does not mean that it is necessary to fit business accounts into a regulation based on consumer products.

(5) Red Flag. The Agencies propose to define "Red Flag" as a "pattern, practice, or specific activity that indicates the possible risk of identity theft." We strongly recommend that the Agencies qualify this definition by deleting "possible risk" and inserting, "significant possibility" of identity theft.

Identifying and using Red Flags based on the "possible risk" of identity theft would be extremely time-consuming and expensive because of the high volume of false positives and typical manual review and other expensive measures required to review and resolve. It simply would divert important resources away from effective fraud detection and prevention tools.

Just about any activity or transaction connected to an existing account and the process of opening a new account could be interpreted as a "possible risk of identity theft," requiring financial institutions to detect and take actions. For example, arguably, any time a credit or debit card is used, there is a "possible risk" of identity theft. To reduce fraud, banks could call customers every time they use a bank card and decline the transaction absent the consumer's verification. Equally, card issuers could take weeks to verify information more thoroughly before sending a replacement for a lost credit or debit card, leaving the customer without account access for that period. But surely, neither consumers, nor commerce, would be pleased. Indeed, some customers today complain when a valid transaction is denied because it was identified as suspicious and the bank was unable to verify its validity with the cardholder. It is not possible to eliminate all fraud associated with financial products without eliminating the service or product for all but a few or making the service or product prohibitively expensive. There is always a balance between fraud detection and prevention and consumer convenience and choice.

While the Agencies have indicated in the Supplementary Information their intent that the proposed Regulation be "risk-based," the proposed Regulation itself does little to assure financial institutions that

this is in fact the case. Adopting a wide open standard of "possible risk," in effect, eliminates any risk-based analysis, notwithstanding claims in the Supplementary Information.

The Supplementary Information notes that the use of possible risk "is based on the statutory language."[1] However, the statutory language uses the phrase "existence of identify theft." [2] The Agencies appear to rely on the Federal Trade Commission's interpretation of the term "identity theft,"[3] so that the Red Flags under the proposal are indicators of "the possible existence of a fraud committed or attempted using the identifying information of another without authority." It is not clear how this phrase is then transformed into "possible risk," which is clearly much broader. Accordingly, we do not believe the statutory language supports the proposed use of "possible risk."

A narrower approach is also consistent with the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, which adopts more of a risk-based approach. For example, that Guidance provides that when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information and determines that "misuse of its information about a customer has occurred or is *reasonably possible,* it should notify the affected customer as soon as possible." (Emphasis added.)

To avoid second-guessing by examiners and angst by compliance officers and risk managers trying to interpret and implement the Regulations and anticipate examiners, we strongly suggest that the Agencies make clear that they are promoting a risk-based approach by qualifying that Red Flags relate to the "significant possibility" of identity theft.

(c) Identity Theft Prevention Program.

Under this section of the proposal, financial institutions must have a written Identity Theft Prevention Program ("Program"). "The Program must include reasonable policies and procedures to address the risk of identity theft to its customers and the safety and soundness of the financial institution or creditor, including financial, operational, compliance, reputation, and litigation risk. . ."

We do not believe that it is necessary to have a formal requirement for a separate, written document labeled "Identity Theft Prevention Program." First, it is not required by the statute. Second, financial

---

1 71 Federal Register 40790

2 15 USC 615(e)(2)(A)

3 The statute authorized it to define for purposes of alerts only under Section 603(q)

institutions use an assortment of policies and programs that work together, but need not be packaged in a single source to be successful in fighting fraud.

The proposal also provides that the Program be "[a]ppropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities." We strongly agree. It is critical that the final Regulation recognize that the need for and effectiveness of identify theft and fraud prevention systems will vary significantly by bank size. Many solutions appropriate for the largest institutions are not effective or affordable for other institutions. For example, the largest banks rely on sophisticated systems, both propriety and purchased, to detect check fraud. However, those systems are expensive and require a minimum amount of account and check volume and fraud, in addition to significant human resources, in order to be predictive and effective.

We also strongly recommend that the Agencies add to this section that financial institutions may take into account the cost and effectiveness of polices and procedures and the institution's history of fraud. Otherwise, there is an argument that each of the Red Flags must be applied regardless of its cost or effectiveness or regardless of the fact that the institution has experienced little or no fraud for that particular product. Equally, identity theft prevention and mitigation measures could be demanded without regard to cost or effectiveness. While many of the proposed Red Flags and theft prevention and mitigation measures are effective today, experience has shown that they can become obsolete very quickly as fraudsters adapt and technology improves.

In addition, the proposal provides that the Program must be designed to address changing identify theft risks "as they arise," based on the experiences of the financial institution with identity theft, changes in methods of identity theft, methods to detect, prevent, and mitigate identify them, the types of accounts it offers and business arrangements. Later, in Section (d)(1)(i), the proposal provides that the Red Flags "identified must reflect changing identity theft risks to customer. . .as they arise." The Supplementary information elaborates that this means incorporating Red Flags "on a continuing basis."

While it is important that financial institutions respond to new identity theft techniques and new solutions, these provisions could be interpreted to require an identity theft review on a daily basis, which would require dedicated staff and complicated procedures, a significant burden for all financial institutions, but particularly smaller institutions. We recommend deletion of "as they arise" from both Sections (c)(2) and (d)(1)(i) and deletion of "on a continuing basis" from the Supplementary Information to Section (d)(1)(i). The Agencies could maintain the notion that the Program be updated appropriately but add flexibility by providing

that the Program "be designed to address changing identity theft risks in a reasonable time after they become apparent."

The Supplementary Information further explains that financial institutions must "periodically reassess whether to adjust the types of accounts covered by its Program and whether to adjust the Red Flags that are part of its Programs based upon any changes in the types and methods of identity theft that it experiences." As noted, we agree that it is important to monitor identity theft and fraud and make appropriate adjustments to fraud prevention programs and practices. However, the nature of any examiner-reviewed, board-approved "Program" is that financial institutions have internal administrative processes that make changes slower to occur and render the Program somewhat rigid. The Commentary or Supplementary Information should make clear that changing the Program is not necessary to implement a new identity theft or fraud solution or change an existing one. Otherwise, financial institutions lose the ability to respond quickly to the latest fraud or to adopt the newest solution.

While we do not believe that the Regulation should specify what "periodically" is, the regulation, commentary, or Supplementary Information should allow financial institutions broad flexibility, based on the size of the institution, actual fraud and identity theft experiences, and the nature of products offered, and the risk assessments performed.

(d)(1)(i) Development and implementation of Program:
Identification and evaluation of Red Flags.
Risk-based Red Flags.

Under the proposal, the Program "must include policies and procedures to identify Red Flags, singly or in combination, that are relevant to detecting a possible risk of identity theft. . . using the risk evaluation set forth in paragraph (d)(1)(ii) of this section." The proposal continues, "At a minimum, the Program must incorporate any relevant Red Flags from:

(A) Appendix J,
(B) Applicable supervisory guidance;
(C) Incidents of identity theft that the financial institution or creditor has experienced; and
(D) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks."

The Supplementary Information acknowledges that some Red Flags may be less reliable except in combination with additional Red Flags. We submit that many of the proposed Red Flags are only relevant in combination and often not indicative individually. Indeed, many vendor-provided products incorporate numerous proposed Red Flags and use

sophisticated algorithms to identity the level of fraud risk. To help emphasize that in many cases a combination of Red Flags is more reliable and the risk-based nature of the identify theft and fraud analysis, we recommend adding to paragraph (d)(1)(i) that financial institutions, when identifying and evaluating Red Flags, use a risk-based approach in determining whether a Red Flag or combination of Red Flags is a likely indicator of identity theft or fraud.

The Agencies request comment on whether the enumerated sources of Red Flags are appropriate. Generally, we believe that most are. (See comments to proposed Appendix J.) Our concern is the mandatory incorporation of Red Flags from these sources: "*At a minimum,* the Program *must* incorporate any relevant Red Flags. . ." (Emphasis added.) While the proposal qualifies the requirement with "relevant" Red Flags, the provision in effect imposes a mandatory review, analysis, and report of virtually any new identity theft incident or trend and potential prevention measure, regardless of likely continuation, application, or impact on the financial institution or its customers. In addition, any proposed changes to the Program would have to be officially approved through various channels in order to be incorporated into the Program. This becomes particularly worrisome if the risk-based nature of the analysis, as well as cost and effectiveness of Red Flags and fraud solutions are not also specifically incorporated into the regulation. Accordingly, we suggest that the Agencies delete, "At a minimum, the Program must incorporate any relevant Red Flags" and replace with language similar to that in the Agencies' Information Securities Standards. The Regulation should provide, "Financial institutions and creditors should incorporate any Red Flags they conclude are appropriate."

The Agencies specifically request comment on the anticipated impact of this proposed paragraph on third party computer-based products that are currently being used to detect identify theft. The third-party computer-based products are generally very useful to all financial institutions. They are especially helpful to and relied on by small and mid-size institutions because they provide sophisticated and predictive products based on extensive research, experience, and databases that otherwise would be unavailable. Many incorporate a large number of the proposed Red Flags. However, some products, including "add-ons" are not necessarily cost-effective or justified for some institutions. Absent the above-suggested modification, financial institutions would certainly be pressured by both vendors and examiners as well as the Regulation itself, to purchase additional products, even though those products are not especially effective for a particular institution. The result would be unnecessary expense.

(d)(1)(ii) Risk evaluation.

The proposal provides that in identifying relevant Red Flags, the financial institution *must* consider:

(A) Which of its accounts are subject to a risk of identity theft;
(B) The methods it provides to open these accounts;
(C) The methods it provides to access these accounts; and
(D) Its size, location, and customer base.

While *suggestions* about how to identify relevant Red Flags are useful, we recommend that the Agencies make clear that these are only *suggestions* that financial institutions should *consider*. Many institutions may, in fact, consider these factors, but they may be indirectly factored into an overall design or categorized differently, for example. As a list in an official regulation, however, they become an artificial checklist for the financial institutions and their examiners, requiring financial institutions to reconstitute their approach to the identity theft Program, when doing so does not advance the goals of the Program. Financial institutions should have wide latitude to determine what factors they should consider and how they categorize them.

We suggest that the final Regulation add to the list of suggestions that banks may consider accounts subject to risk of identity theft "based on their identity theft experience." As noted earlier, virtually all types of bank accounts and products are subject to a risk of identity theft, so without modification, this proposed phrase becomes meaningless. For example, if a bank is not experiencing any identity theft related, for example, to home equity lines of credit or business accounts, it should not be required to analyze and document why home equity lines of credit or business accounts generally are not at risk for identity theft. For similar reasons, we suggest that the phrase be modified to read "likely risk of identity theft."

We also suggest that the Agencies make clear in this paragraph that financial institutions may consider, "The cost of using a Red Flag and its effectiveness for that institution." Otherwise, financial institutions will be spending valuable resources for solutions that may not be cost-effective, or even effective, potentially at the expense of other solutions not on the official Red Flag list. Fraudsters and fraud are dynamic, constantly changing, as must the detection methods and solutions. Systems become obsolete as fraudsters decode them (or, for example, read the Regulation). Financial institutions should not be pressured or required to implement or continue using identity theft and fraud detection systems that are marginally effective or unduly expensive.

For similar reasons, this paragraph should make clear that financial institutions are also permitted to use a risk-based analysis in identifying which Red Flags are relevant. While paragraph (d)(2)(iv) provides that financial institutions should "address the risk of identity theft,

commensurate with the degree of risk posed. . .” this only goes to the identity theft prevention and mitigation, not to the selection of relevant Red Flags.

(d)(2) Identity theft prevention and mitigation.

The proposal requires that the Program include “reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account. . .“ A list of mandatory measures follows. The first in the list is the requirement to obtain identifying and verifying information about a person opening an account. The Regulation specifically provides that a financial institution that uses the policies of the CIP requirements of the USA PATRIOT Act under these circumstances satisfies this requirement. We strongly support this provision, which is consistent with the language and spirit of the statute, and encourage adoption of the exemption provisions of the CIP regulations for consistency in implementation of both regulatory mandates. There is simply no reason to unnecessarily add duplicate and burdensome rules.

Proposed paragraph (iii) requires that financial institutions assess whether the Red Flags “evidence a risk of identity theft.” It continues, “An institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft.”

We strongly recommend deletion of this sentence. In effect, mandatory review and analysis of each and every Red Flag will require creation of an entire department dedicated to the project. It is simply unnecessary and a waste of valuable resources for financial institutions to divert limited resources to such a time-consuming administrative exercise focused on reviewing and documenting and re-reviewing and re-documenting the obvious. Financial institutions already have sufficient incentives to develop, implement, and refine identity theft and fraud prevention programs as they generally suffer any financial loss, but also contend with potential customer relations and public relations fall-out.

In any case, for reasons discussed with regard to the definition of “Red Flag,” if the sentence is retained, it should read, “An institution or creditor must have a reasonable basis for concluding that a Red Flag does not evidence a significant risk of identity theft.” As discussed earlier, virtually any activity related to a financial account could pose a “risk of identity theft.” Similarly, a positive Red Flag could indeed show a risk of identity theft, and most likely does – presumably, that is why it is a Red Flag. To be consistent with the Agencies proclamations in the Supplementary Information, the Regulation should reflect a risk-based approach.

The Supplementary Information offers guidance on what might be a "reasonable basis" for concluding that a Red Flag does not indicate identity theft or fraud. For example, it offers, patterns of spending that are inconsistent with established patterns of activity because the customer is traveling abroad might be a reasonable basis for concluding that a Red Flag does not indicate identity theft. However, this could suggest that if a customer has not informed the financial institution of the customer's travels or the bank otherwise has no actual knowledge of this fact, it should decline the transaction because there is a risk of identity theft. The financial institution could be challenged for not declining the transaction (if it made the wrong decision). Yet, customers could be greatly inconvenienced, at a time and place when they most need access to their account. Moreover, it suggests that institutions should not decline foreign transactions if the customer has informed them they are traveling abroad. In some cases, the out-of-pattern detection systems cannot simply accommodate individual accounts or individual customer activities. We recommend that the Agencies avoid specific examples, which may become obsolete, and instead stress the risk-based nature of the analysis and the institutions' broad discretion in making a decision.

(d)(2)(iv) Address the risk of Identity Theft.

This paragraph requires financial institutions to "address the risk of identity theft, commensurate with the degree of risk posed. . ." it then lists actions to be taken. We strongly agree that the risk be addressed "commensurate with the degree of risk posed," which supports the critical risk-based approach. We suggest that to emphasize this point, the Agencies incorporate into the final Regulation the words contained in the Supplementary Information that the list is a list of measures that a financial institution "may take depending on the degree of risk that is present."

According to (F) in the list, financial institutions should consider "closing an existing account." The Supplementary Information adds additional information, noting, "[i]f the financial institution . . is notified that a customer provided his or her password and account number to a fraudulent website, it likely will close the customer's existing account and reopen it with a new account number." We strongly object to including this in the Supplementary Information because, in effect, it becomes mandatory, as examiners will demand strong arguments and evidence why the financial institution should not close the account. Yet, financial institutions today already have other tools and controls to address these situations that eliminate the risk but avoid inconveniencing customers by closing an account. If an account must be closed, customers may lose temporary access to their account and have to notify numerous payees of preauthorized transactions connected with that account or card. We should assume that other effective and more convenient controls will develop and be used more widely. Moreover, since financial institutions are generally liable for any fraud losses, they already have sufficient

incentive to ensure that the account and funds are protected. To avoid etching in stone solutions that may become obsolete, we recommend deletion.

Included in (H) of the list of measures an institution may take is "declining to issue an additional credit card when the financial institution or creditor detects a fraud or active duty alert associated with the opening of an account or an existing account." We recommend that this be deleted as it would rarely, if ever, be applicable and would only serve to confuse.

Typically, a consumer report, which is the means for learning of an alert, is not pulled when a financial institution issues an additional credit card for an existing account, so the proposal has little application to existing accounts. In addition, if the financial institution learns of an alert at account opening, it will choose, based on further investigation, either to open the account or not. If it chooses to open the account because it has validated the applicant's identity, it is not clear why it cannot issue "additional cards" if the applicant has so requested. The Agencies note that the proposed (H) reflects Section 112 of the FACT Act related to alerts, a section separate from the section related to the Red Flags. Given that it is a separate and distinct section related to alerts, we do not believe that it is necessary to enshrine it in Red Flag Regulations or guidelines, especially as it is pretty useless. Though it would rarely ever be applicable, if retained, financial institutions would still have to puzzle over what to do with it and document to examiners why it they are not applying it. Accordingly, it should be deleted.

(d)(3) Staff training.

This paragraph requires financial institutions to train staff to implement its Program. It is not clear why staff training is specifically required under this Regulation as opposed to other regulations, absent a specific statutory requirement. Doing so suggests that this Regulation is more important than the other dozens of regulations, including other consumer protection regulations, with which financial institutions must comply. We simply see no justification to elevate it above all the other important consumer protection regulations or other regulations absent Congressional intent. Moreover, given that financial institutions are generally responsible for identity theft losses and have a vested interest in customer service, they have sufficient incentives to ensure that appropriate staff is trained.

In addition, the Supplementary Information specifically provides the example that staff should be trained to notice "anomalous wire transfers in connection with a customer's deposit account." This goes far beyond the statutory language or intent and imposes a huge burden on tellers and other staff, already bogged down with learning dozens of complicated regulations in addition to the basic responsibilities of providing banking

services to customers. For these reasons, many of these types of decisions and Red Flags are incorporated into automated systems or made in the back office. Given that the customer is generally not liable if the transaction was not authorized, it is also not necessary. However, it potentially imposes a significant and unintended liability on banks: customers and law enforcement will use the Regulations to support claims that the banks are responsible for authorized transactions to fraudsters. For example, assume a fraudster sends counterfeit cashiers' checks to consumers. It could be that the fraudster is pretending to purchase an item advertised online and is overpaying the seller and asking that the seller wire the excess to another account. Or the fraudsters might inform the targets that they have won a lottery in a foreign country or that they have inherited money from an unknown relative outside the U.S. However, in order to collect the inheritance or lottery proceeds, they must wire funds, e.g. taxes, to a specified bank account, typically out of the country. The bank, under Regulation CC, must provide the funds, even though it does not yet know that the check is counterfeit. The check returns after the funds are withdrawn or wired. In this case, the customer is in the best position to evaluate the situation and risk and the bank, by law, cannot prevent the customer from withdrawing funds. Yet, customers and some law enforcement have asserted that the bank or teller "should have known" that the check deposit or withdrawal was unusual. In fact, banks do not have systems that can detect these transactions because they fall outside the usual fraud filter parameters. However, customer and law enforcement could use the language in the proposed Regulation and Supplementary Information to support a claim that it was the bank's responsibility to detect that an *authorized* transaction was being made to a fraudster, even though it has nothing to do with identity theft. In recent years, banks have complained that customers are using a similar argument to avoid liability based on the fact that banks are required to detect, identify, and report suspicious activities. For these reasons, the Agencies should omit this reference.

(d)(4) Oversee service provider arrangements.

Under the proposed paragraph, financial institutions who engage service providers to perform an activity on its behalf, and the requirements of its Programs are applicable, the financial institution must take steps designed to ensure that the activity is conducted in compliance with a Program that meets the requirements of (c) and (d).

The Agencies also ask whether it is necessary to address service provider arrangements in the Red Flag Regulation, or whether it is self-evident that a financial institution remains responsible for complying with the standards set forth in the Regulation, including when it contracts with a third party to perform an activity on its behalf.

We agree that financial institutions are responsible for compliance with the Regulation, but believe it unnecessary to put in the Regulation. The Agencies should recognize, however, that vendors may not necessarily reveal all the details of their proprietary systems. For example, some vendors create "risk scores," which incorporate various factors to measure the relative degree of risk of identity theft and fraud. The vendors may not provide the specific reasons, in order to protect their proprietary product, but also to prevent fraudsters from using the information to circumvent their system. The Commentary or Supplementary Information should therefore allow flexibility in allowing financial institutions to determine whether a vendor product satisfies the Regulation.

(d)(5) Involve the board of directors and senior management.

The proposal requires that the board of directors or an appropriate committee of the board approve the Program. In addition, it requires the board of directors, an appropriate committee of the board, or senior management to oversee the development, implementation, and maintenance of the Program. Finally, staff responsible for the implementation of the Program must report to the board, an appropriate committee of the board, or senior management, at least annually, on compliance by the financial institution.

ABA opposes any requirement or regulatory "suggestion" that the board of directors or board committee approve the Program or receive special annual reports. First, we believe that it will slow down implementation and delay appropriate and necessary modifications to Identity Theft Programs. By nature, programs requiring board or board committee approval require extensive documentation and very deliberate drafting and are slow to reach approval. Yet, also by nature, fraud and identity theft pop up quickly, sometimes unexpectedly, and often require a quick and nimble response. Requiring boards or their committees to review annual reports and approve Programs will slow Program implementation, delay appropriate modifications, hamstring institutions' ability to respond quickly to the latest scam or technology, and increase the risk of identity theft and fraud. This compares to CIP requirements and customer data protection which are far narrower in scope and tend to be more static.

Second, preparation for document approval by boards is not only time-consuming, it is expensive. Banks report high costs for example, for preparing reports and documentation required by Gramm Leach Bliley Act. In addition, boards and board committees of financial institutions are already overburdened with review of regulatory compliance. Over time, this tendency to pile on will gradually reduce time for important core-business considerations.

Finally, absent a Congressional directive, we do not believe that the Agencies should assume that the Red Flag guidelines are more important than other regulations. Unlike some other statutes, the Red Flag provisions of the FACT Act do not contain a requirement for board of director involvement in the Red Flag guidelines. Yet, the Agencies are elevating the proposed Regulation above other important regulations absent any Congressional directive, which Congress gives when it believes it to be appropriate. The Agencies should exercise some restraint and discretion and defer to Congress about the relative importance of various statutes. Otherwise, boards may have to review and approve compliance with every regulation and program, potentially at the expense of those designated by Congress as meriting this special attention.

__91. Duties of card issuers regarding changes of address.

This section implements the specific FACT Act requirement that Agencies prescribe regulations requiring credit and debit card issuers to assess the validity of change of address request. Specifically:

> A card issuer must establish and implement reasonable polices 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, an additional card may not be issued unless the cardissuer takes certain steps:

> Notifies the cardholder of the request at the cardholders' former address and provides the cardholder a means or promptly reporting incorrect address changes;
>
> Notifies the cardholder of the request by any other means of communication that the card issuer and the cardholder have previously agreed to use; or
>
> Uses other means of assessing the validity of the change of address in accordance with policies and procedures established in connection with section 41.90

We suggest that the Agencies either in the Regulation, Commentary, or Supplementary Information specifically provide that financial institutions, as one alternative, may comply with the provision if they verify the address at the time of the address change request, whether or not the request is linked to a card request. Similarly, financial

institutions should have the option to simply verify addresses any time an additional card is requested, regardless of whether there has been a change of address request. These procedures are more protective than only verifying the address change when it is linked with a card request.

Many institutions do not link an address change request with a card request and it is not clear whether this remains a significant indicator of fraud. While it might have been so at one time, it appears that fraudsters have shifted from using this technique, thwarted by fraud prevention procedures.

It is also important that the Regulation allow broad leeway in allowing financial institutions to verify address changes. Currently, financial institutions use a variety of means to verify address changes and those methods change and will continue to change. For example, some have made adjustments based on complaints from abused spouses who have changed addresses. Spouses have them then located through the address verification notice. The Regulation, Commentary, or Supplementary Information should also specifically allow financial institutions to verify the address change through verification of the customer's identity. In some cases, this may be the most effective verification of the address change and one recognized under CIP.

Effective date.

We strongly recommend that the Agencies provide institutions at least 18 months to comply with the final Regulation. The final Regulation will require the involvement of multiple levels of the organization and multiple disciplines that may not otherwise have frequent interaction. In addition, technological solutions will play an important role in implementing the Regulation. Small institutions particularly will face challenges internally and with vendors in understanding, selecting, and implementing software and other changes. Moreover, information technology projects are scheduled far in advance. Inserting any major project that disrupts those schedules is costly, as resources must be diverted and projects rescheduled.

Attachment B

APPENDIX J TO PART 41 – INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION
Red Flags in Connection with an Account Application or an Existing Account Information from a Consumer Reporting Agency

2. A notice of address discrepancy is provided by a consumer reporting agency.

The Agencies should clarify that the same definition of notice of address discrepancy under Section __82(b) applies here. That definition describes a discrepancy as a "substantial difference between the address provided by the user and the address in the report, ensuring the discrepancies due to "fat fingers" or typographical errors are not covered.

3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries.

b. An unusual number of recently established credit relationships.

c. A material change in the use of credit, especially with respect to recently established credit relationships.

d. An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

We strongly recommend that this proposed Red Flag be deleted. We are not aware of any data or models which demonstrate these factors to be reliable indicators of identity theft. What is "significant increase" in the volume of inquiries, an "unusual number" of recently established credit relationship, a "material change" in the use of credit absent data demonstrating a connection to identity theft? Using them to measure risk of identity theft would generate too many false positives to be useful, because more often than not, such factors are indications of financial stress or lack of creditworthiness. The models that use this information to measure creditworthiness cannot be assumed to be, and in fact are not likely to be, the same as those that might, if at all, measure the risk of identity theft.

It is not clear then what a financial institution could do if it is alerted that these factors exist; it cannot reasonably discern whether they are due to financial difficulties or identity theft. However, if it makes an adverse

action based on the information in the consumer report, it must notify the consumer, who will presumably know the reasons for the reported information and respond appropriately. Accordingly, the current system already alerts the consumer to any problem, if, in fact, there is one.

Moreover, this Red Flag assumes that all consumer reports obtained are specifically reviewed. In many cases, creditors rely on the credit score and only review the actual report if, for example, it is a borderline case. Even if a financial institution does review the account, the number of inquiries, for example, may be the result of the consumer shopping for a car or home. We are not aware that these types of inquiries are filtered from the report sent to the users as they are for credit scores.

Documentary Identification

7. *Other information on the identification is not consistent with information that is on file, such as a signature card.*

Our concern is that this provision could be interpreted to apply in circumstances when it is not practical or appropriate, e.g. a credit card transaction. The Agencies could clarify that it should be considered when information is readily available or accessible. In addition, we suggest that the Agencies add "or recent check" after "signature cards" to reflect some institutions' practices with regard to check cashing.

Personal Information

10. Personal information provided is associated with known fraudulent activity. For example:

> *a. The address on an application is the same as the address provided on a fraudulent application; or*
> *b. The phone number on an application is the same as the number provided on a fraudulent application*.

The final Regulation should make clear that the Agencies do not envision financial institutions necessarily maintaining their own warehouses of "bad" addresses and phone numbers. For a variety of reasons, financial institutions do not maintain centralized databases of "bad" addresses or telephone numbers. Not only are individual affiliate databases separate, individual product databases within a single entity may also be separate. The separate platforms are due to mergers, type of product or affiliate development, type of product, and other reasons.

Moreover, card networks, for example, provide such databases for card issuers, and other databases might be available from third party vendors. These databases may be more reliable and effective and less

costly than individual company databases as the volume of information collected would make them more robust.

11*. Personal information provided is of a type commonly associated with fraudulent activity. For example:*

a. The address on an application is fictitious, a mail drop, or prison.
b. The phone number is invalid, or is associated with a pager or answering service.

The final Regulation should make clear that financial institutions may rely on third-party vendors for these types of investigations, where their use is appropriate. Agencies should also indicate that it is acceptable for a financial institution to use a third party vendor system in which such factors are embedded, but which only informs the financial institution generally, e.g., "address does not match" and not necessarily with specifics. However, the information is sufficient to prompt the financial institution to investigate further.

We also suggest deleting "associated with a pager or answering service." First, it provides a useful hint to fraudsters, who will simply use other options. Second, it is not clear that this will continue as a reliable indicator of identity theft because more people are using such products for perfectly legitimate purposes, just as cell phones at one time served as an indicator of possible fraud, but are not longer considered such.

Also, the Agencies should recognize in the Commentary or Supplementary Information that "invalid" phone number does not include inadvertent typographical errors.

12. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customers.

We suggest that this Red Flag be deleted. Financial institutions already use sophisticated and effective systems designed to verify name, address, and Social Security Number. A separate internal database would add little, as there are many valid reasons customers have the same address and phone number: they are related or for other reasons share the same residence. Financial institutions even report that some wives still use their husbands' Social Security numbers. Also, as noted in comments to proposed Red Flag number 10, systems currently do not permit financial institutions to verify in an automated fashion such information across affiliates or even product lines.

13. The person opening the account or the customer fails to provide all required information on an application.

We suggest that this Red Flag be modified to clarify that "required" information means information required for identification purposes, such as CIP related information: name, address, Social Security Number, and date of birth. Financial institutions may require other information for reasons unrelated to customer identification that failure to provide would not suggest identity theft or fraud.

14. Personal information provided is not consistent with information that is on file.

We recommend that the Agencies clarify that "provided" means "provided by the person seeking to access or open the account" to avoid ambiguity that it might be referring to another source. We also suggest that the meaning of "file" be clarified as "the file associated with the account subject to the inquiry." Otherwise, it could be interpreted to mean all files across product lines and affiliates. Checking all files across product lines and affiliates may not be practical or feasible for the reasons discussed in comments to Red Flag number 10. We also suggest the Agencies clarify that "personal information" means CIP items: name, address, date of birth, and Social Security Information. While many institutions may validate other personal information, based on experience and available programs, financial institutions will not know how to interpret such a broad term, limiting its effectiveness as guidance, especially if the final Regulation does not make clear the risk-based nature of analyzing and using Red Flags.

15. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

We suggest that the Agencies revise this provision to reflect the more widespread use of "challenge" questions collected after customer identification and account opening in order to authenticate an existing customer seeking to access or use an account. Usually, at account opening, financial institutions do not have information beyond information contained in a wallet or consumer report. Once the customer's identification has been verified and the account opened, they may collect additional information from the customer that is not found in a wallet or consumer report and use "challenge" questions based on this information to validate customers when they are seeking access to an account.

Address Changes

16. Shortly following the notice of a change of address for an account, the institution or creditor receives a request for new, additional, or replacement checks, convenience checks, cards, or a cell phone, or for the addition of authorized users on the account.

As with proposed Section __.91 regarding debit card and credit card requests made shortly after an address change request, the Agencies should make this Red Flag more flexible and make clear that if other measures are used to avoid such fraud, it is not necessary to consider the link between the address change request and request for card or check. Most financial institutions do not link a change of address request to subsequent requests for credit or debit cards or checks. Rather many for example, verify the address change at the time of the address change request or card request. We believe that financial institutions should have the flexibility to consider these and other options. We also suggest deleting the reference to checks because the connection between an address change and request for new checks soon after is not a good indicator of fraud: it is common for people who move to request new checks with the new address printed on them at the same time. Accordingly, there will be a high volume of false positives.

17. Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with the customer's account.

It is not clear how returned mail intended for an existing customer is a reliable indicator of identity theft or risk of identity theft. The only danger appears to be when mail is intercepted -- in which case it would not be returned. Accordingly, this should be deleted.

In any case, if retained, this Red Flag should reflect that it is not referring to a single return of mail as a single return. Mail can be returned for a variety of valid reasons: the customer has moved without notifying the financial institution, a common occurrence; the U.S. Postal Service mis-delivered it and the recipient returned it; the address was entered incorrectly into the financial institution's system. Accordingly, if retained, the final Red Flag should refer to mail "repeatedly returned."

If retained, the Red Flag should also indicate that it is only referring to mail containing specific financial information related to an account. Returned marketing materials, for example, would not appear to pose a risk.

In addition, the Red Flag should be modified to include only "paper mail." Customers close e-mail accounts frequently without notifying financial institutions. And a change in an e-mail account does not present the same risk as a change in physical address.

Anomalous Use of the Account

18. A new revolving credit account is used in a manner commonly associated with fraud.

For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

We do not believe that this Red Flag is particularly helpful or effective and recommend that it be modified to be far more general or deleted. Fraudsters, as they learn how card issuers identify suspicious activity, simply adjust their patterns: instead of purchasing jewelry or electronics from a specialized retailer, they make the same purchases at a department store, in which case the issuer does not know the nature of the purchase. Or, as card issuers have observed, fraudsters have learned to make timely payments (over the minimum) over a period of time, and then either "bust out," suddenly making large purchases, or defraud more subtly, making larger purchases gradually, until they default -- all strategies intended to circumvent fraud filters. The Agencies should avoid this type of detail in the Regulation and Appendix as these types of specific Red Flags invariably become obsolete and only serve as useful tips to fraudsters, which of course hastens their path to obsolescence. Instead, the Agencies should allow financial institutions maximum flexibility to learn and respond quickly and effectively as fraudsters adapt to the latest fraud filters.

In any case, this Red Flag should not apply to home equity lines of credit as it would not be particularly helpful for this product. Unlike the credit card systems which rely on merchant codes to identity the type of merchant, no such system allows financial institutions to necessarily know the nature of the payee receiving a home equity line check, let alone capture that information in an automated fashion in order to monitor. Financial institutions rely on other types of controls to guard against unauthorized transactions on home equity lines of credit, which they have an incentive to use as they are generally responsible for any such transactions.

19. An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

Certainly, many financial institutions use systems to detect unusual activity on financial accounts, card issuers being the most frequent users of the most sophisticated systems. In addition, the largest institutions also effectively use systems to detect out of pattern activities for deposit accounts. Others, depending on the institution and type of product and transaction, use other types of controls. For example, they may identify and review risky transactions, not based on typical account activity, but on the *general type* of transaction, e.g., large dollar transfers, online payments to an individual, foreign ATM transactions. Or, they may prohibit certain types of transactions entirely. It is important that the Agencies recognize these controls as appropriate and effective alternatives.

Examiners should understand that systems to identify unusual activity will probably not be appropriate for many institutions because of the limited risk in these situations, the expense of the programs, the significant and continuing investment of human resources to monitor, review, and investigate exception items or hits, as well as tweak systems continuously to minimize false positives and maximize good hits. ABA has over the years approached vendors about more affordable and suitable deposit account fraud filters for institutions that are not among the largest, with little success. Only the largest institutions should be expected to use them.

We are also concerned that absent an explicit recognition by the Agencies that they are not suitable for all institutions, that reasons similar to those discussed in comment to proposed Section __(d)(3) related to staff training about Red Flag Programs, this Red Flag in particular could be used to support suits asserting that banks should be responsible for authorized and intentional transactions made in connection with fraudulent scams even though the banks are not in a position to detect and warn the consumer. This proposed Red Flag is another example of why it is important for the Agencies to stress the risk-based nature of the Red Flag analysis.

Notice from Customers or Others Regarding Customer Accounts

23. The financial institution or creditor is notified that the customer is not receiving account statements.

The Agencies should clarify that this refers to “paper statements,” and does not include electronic statements. There may be a myriad of reasons, usually technical, that electronic statements may not be not delivered, rarely having anything to do with fraud.

24. The financial institution or creditor is notified that its customer has provided information to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website.

We suggest that the Agencies specify that the "information" they are referring to is "information related to an account held by the financial institution." This would include account numbers, passwords, etc.. However, if the information is unrelated to the financial institution, there is little that financial institution can do. To avoid ambiguity, it should be clarified.

Other Red Flags

26. The name of an employee of the financial institution or creditor has been added as an authorized user on an account.

Financial institutions report that they are not aware of systems that monitor and detect when any employee's name has been added to an account held by the financial institution. Typically, the addition of the employee's name is detected after an account has been flagged for other reasons, e.g. an inactive account has become active. Accordingly, the Commentary or Supplementary Information should recognize that institutions are not expected to monitor for such activity on a broad scale.

27. An employee has accessed or downloaded an unusually large number of customer account records.

Financial institutions report that they are not able to detect in a practical manner whether employees have accessed or downloaded an unusually large number of customer account records, but some monitor for large e-mails, though often only if the employee is already under suspicion. We suggest that the Agencies modify the proposed Red Flag to, "An employee has sent e-mails containing unusually large attachments."

28. The financial institution or creditor detects attempts to access a customer's account by unauthorized persons.

We are concerned that this could be interpreted to impose special broad requirements to detect unauthorized account access. Financial institutions rely on a variety of controls to prevent unauthorized access, but if they successfully prevent it, for example, by declining the transaction, so both customer and financial institution are protected, are they required to do more based on this Red Flag? Moreover, there is a balance: customers and employees responding to customers also need to access accounts.

29. *The financial institution or creditor detects or is informed of unauthorized access to a customer's personal information.*

The Red Flag should clarify that "personal information" is "personal information held by the financial institution." It should be clear that it is not the responsibility of a financial institution to notify customers about another party's breach or to expose them to liability for claims that they should have.

30. There are unusually frequent and large check orders in connection with a customer's account.

We recommend deletion of this Red Flag. While check vendors may be set up to call in about an unusual request, financial institutions report that they have rarely if ever received such a notice, suggesting that this is not a technique used by fraudsters. Moreover, it is not clear why ordering an unusually high number of checks would be more useful to fraudsters than ordering the standard number, which is probably sufficient for their purposes before they get detected. It is more likely that actual check transaction volume would be a better indicator. We suggest deleting this as we do not believe it to be an indicator of identity theft or fraud.

31. The person opening the account or the customer is unable to lift a credit freeze placed on his or her consumer report.

We strongly recommend deletion of this proposed Red Flag. It is not clear how the Agencies expect financial institutions to know that the applicant is unable to lift a credit freeze or what the Agencies expect them to do if they do learn of it.

If the financial institution is unable to obtain a consumer report due to a freeze and informs the applicant, and the applicant does not follow up by removing the freeze and contacting the financial institution, the financial institution cannot know whether the applicant simply changed his or her mind or the applicant was unable to remove the freeze.

Moreover, it is not clear what action the financial institution can or should take in this instance. If a fraudster was involved, the system worked: no account was opened and that should be the end of it. It is not clear what following up with fraudsters would accomplish except to alert them that they should endeavor to get the freeze lifted, which if "friendly fraud" (i.e., someone know to the victim) is involved, could be achieved.

Legitimate applicants will follow up, it they continue to be interested in the product. It should not be incumbent on the financial institution to determine the applicant's mind.