JPMorganChase

Andrea Beggs
Senior Vice President
Office of the General Counsel

September 18, 2006

Office of the Comptroller of the Currency
250 E. Street, SW
Public Reference Room
Mail Stop 1–5
Washington, DC 20219

Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attn: Regulation Comments
Chief Counsel's Office
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, VA 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: 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 Project No. R611019

Ladies and Gentlemen:

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") have requested comments on their proposed regulations related to implementation of Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. 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 (the "Proposed Rule"). JPMorgan Chase & Co., on behalf of JPMorgan Chase Bank, National Association, its lead subsidiary bank, Chase Bank USA, National Association, its credit card bank, and its other subsidiaries, appreciates the opportunity to submit this response.

JPMorgan Chase & Co. (NYSE: JPM) ("Chase") is a leading global financial services firm with assets of $1.2 trillion and operations in more than 50 countries. The firm is a leader in financial services for consumers and businesses, investment banking, commercial banking, asset and wealth management and private equity. Under the JPMorgan and Chase brands, the firm serves millions of consumers in the United States and many of the world's most prominent corporate, institutional and government clients. Information about the firm is available on the Internet at www.jpmorganchase.com.

SUMMARY

Chase commends the Agencies for their recognition that an effective identity theft program should be risk-based. The Proposed Rule, however, describes a far more rigid approach that will significantly hamper development and implementation of the innovative systems necessary to prevent fraud. We believe that financial institutions should have the ability to develop a flexible, risk-based program that will focus resources on the most beneficial and efficient strategies to thwart identity theft. We also have specific concerns about the proposed new requirements for reconciling address discrepancies with consumer reporting agencies and the duties of card issuers to verify new addresses.

§ __.90 DUTIES REGARDING THE DETECTION, PREVENTION, AND MITIGATION OF IDENTITY THEFT

§ 615(e) of the Fair Credit Reporting Act ("FCRA") directs the Agencies to establish and maintain guidelines for use by each financial institution and creditor regarding identity theft with respect to account holders at, or customers of, such entities. The Agencies must also prescribe regulations requiring each institution to establish reasonable policies and procedures for implementing the guidelines. The Proposed Rule, according to the Agencies, is intended to provide a "flexible, risk-based approach" that is similar to the guidelines issued under the Gramm-Leach-Bliley Act pertaining to information security (the "Information Security Guidelines"). Chase is pleased that the Agencies intend for the Proposed Rule to be flexible, risk-based, and similar to the Information Security Guidelines. We strongly urge the Agency to maintain these objectives when formulating the final rule (the "Final Rule"). As we discuss in more detail below, however, we believe the Proposed Rule should be revised in order to achieve the goals established by the Agencies.

§ __.90(b) Definitions

Definition of "Red Flag"

The Proposed Rule uses and defines the term "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.

The Supplementary Information released with the Proposed Rule suggests that the Agencies intend to define this term very broadly, noting that it includes circumstances where there is only a risk of identity theft, even if the possible existence of identity theft is not indicated. Unfortunately, this definition is so broad that it is virtually limitless. Almost every transaction with a financial institution has a "possible risk" of identity theft because there is always a risk that identifying information is being used without authority to commit fraud.

As defined in the Proposed Rule, the submission of a loan application, the use of a credit card or debit card and the opening of a deposit account are all Red Flags, because each of these specific activities could involve a possible risk of attempted misuse of a person's identifying information to commit a fraud. To reduce the possible risk of identity theft, financial institutions could call customers every time they use a credit or debit card and decline the transaction absent the consumer's verification. 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. Neither consumers nor commerce would be pleased with such a program. 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. Therefore, a Red Flag should not be defined simply as an activity with a possible risk of identity theft, but should only include those activities that pose a significant risk.

Definition of "Account"

The proposal defines "account" broadly to include asset accounts and extensions of credit for business purposes, as well as for personal, family or household purposes. We believe that business accounts should be excluded. Most of the proposed Red Flags have little if any application to business account fraud. 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 a business. Nevertheless, under the Proposed Rule, financial institutions would have to analyze, document, and periodically review 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 than consumer identity theft for a number of reasons. Financial institutions perform different due

diligence when opening a business account for reasons other than identity theft; they must confirm the viability of the business and rely on information other than a consumer report. In many instances, corporate 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 businesses will use the Red Flags as a means to attempt to avoid responsibility for fraudulent losses, even though the businesses may be in a better position to prevent many types of fraud. This is especially true, given that the broad definition of "identity theft" includes any potentially fraudulent transaction on any existing financial account. For example, businesses could use the Final Rule as a basis to assert that the financial institution should have detected fraudulent transactions by a dishonest bookkeeper because the transaction was an "unusual" transaction. Such an approach moves toward absolving businesses from performing due diligence in hiring employees and monitoring accounts. Already, financial institutions report that businesses are using Suspicious Activity Report requirements in attempts to shift liability and responsibility to financial institutions. We do not believe that the Proposed Rule was intended or should be used to relieve businesses of their current responsibilities related to fraud prevention and detection.

Including businesses in the Proposed Rule is also inconsistent with the approach taken in the Information Security Guidelines, which apply only to information about consumer customers. To the degree that the requirements of the Proposed Rule and the Information Security Guidelines dovetail, as the Agencies suggest that they do, we believe that the definitions should be consistent in order to minimize compliance complexity and burdens. Otherwise, it becomes more complicated to design policies and procedures to comply with both regulations.

§ __.90(c) Identity Theft Prevention Program

The Proposed Rule would require financial institutions to implement a written Identity Theft Prevention Program (the "Program") that must include reasonable policies and procedures to address the risks of identity theft to its customers and the safety and soundness of the financial institution. The Program must address the financial, operational, compliance, reputational and litigation risks of identity theft.

We believe the Agencies can achieve their stated goals if the Final Rule reflects an approach that is more consistent with the approach embodied in the Information Security Guidelines. The Information Security Guidelines require a comprehensive written program that is designed to meet certain objectives. In developing a security program, a bank must identify reasonably foreseeable threats, design a program to control those threats, and adjust the program as appropriate. The Information Security Guidelines constitute a fairly simple requirement that has worked well. We urge the Agencies to use this approach with respect to their obligations under § 615(e) of the FCRA.

We strongly recommend that the Agencies add a provision that financial institutions may take into account the cost and effectiveness of polices and procedures and the financial institution's history of fraud. Otherwise, there is an argument that each of the Red Flags must be applied regardless of its cost, effectiveness or applicability to a particular product or delivery channel, or regardless of the fact that the institution has experienced little or no fraud for that particular product or delivery channel. As a result, 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.

The Supplementary Information further explains that a financial institution 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 Program based upon any changes in the types and methods of identity theft that it experiences." 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 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.

§ __.90(d) Development and Implementation of Program

Chase believes that this is the most important provision of the Proposed Rule. We also believe that this provision should be revised to reflect better the Agencies' intent to adopt an approach similar to that in the Information Security Guidelines, providing financial institutions with the ability to design a flexible and risk-based Program. In order to do so, the Agencies should revise § __.90(d) to build from the objective provided in § __.90(c) to adopt reasonable policies and procedures to address the risks of identity theft. The Final Rule should provide a financial institution with an outline of issues that should be considered in developing its Program without requiring specific approaches. For example, the Final Rule could direct financial institutions to consider issues relating to identification verification procedures at account opening, transaction monitoring and verification, risks associated with Internet communication with consumers, or similar items, but it should not require the financial institution to take specific actions on a transaction-by-transaction basis. This is the approach taken in the Information Security Guidelines. Chase requests the Agencies to take a similar approach in the Final Rule.

§__.90(d)(1) Identification and Evaluation of Red Flags

The Proposed Rule requires a financial institution's Program to include policies and procedures to identify any risk of attempted fraud associated with various accounts. We believe this is too broad. It is not productive, nor do we believe it was the Agencies' intent, to require

policies and procedures to identify all potential risks, no matter how remote or insignificant they are, even if they may be relevant to a type of account or transaction. Yet that appears to be the plain language requirement of the Proposed Rule. 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 other expensive measures required to review and resolve. Such a program would divert important resources away from effective fraud detection and prevention tools.

Financial institutions should be permitted to rely on their own experiences with identity theft. Although the Agencies may choose to provide a list of possible Red Flags, either as part of the Final Rule or as a part of future guidance, these items should be considered illustrative only and not a de facto checklist for financial institutions or examiners. We suspect that many, if not most, financial institutions will be in a better position to determine which risks should be addressed and how to address those risks, than the Agencies. We also do not believe it is necessary to require financial institutions to address subcategories of risk, such as litigation or reputational risk. The goal is to prevent identity theft, regardless of whether the resulting harm is financial or operational.

The Proposed Rule also requires a financial institution to include in its Program a list of "relevant" Red Flags, such as those provided by the Agencies in the Appendix, those identified in any applicable supervisory guidance, and incidents of identity theft that the financial institution has experienced. We urge the Agencies to delete this requirement. Institutions should be permitted to assess which Red Flags are appropriate for their risk-based Programs without the risk of being second guessed by examiners or others who use the Appendix or existing guidance as a presumptive checklist. This will become more difficult as new Red Flags are added to the Appendix and included in supervisory publications over the years.

§ __.90(d)(1)(ii) also requires each financial institution to conduct a "risk evaluation". The "risk evaluation" described in the Proposed Rule, however, is not a true risk assessment for purposes of determining where to dedicate limited resources. Rather, the Proposed Rule would require institutions to consider various account or transaction properties when identifying any risk of fraud that could be associated with them. In order for the Program to be truly risk-based, a financial institution should assess the likelihood and the magnitude of the risks presented, not just enumerate such risks.

It is also important to note that the items listed in the "risk evaluation" portion of the Proposed Rule are not necessarily the ones actually used by financial institutions to identify risks. Financial institutions generally do not design a program to address identity theft by systematically considering the methods used to open and access accounts, or the institution's size, location and customer base. They evaluate risk by analyzing the number and severity of incidents of a certain type and the cause of the associated losses. To require the evaluations described in this subsection would require many financial institutions to develop entirely new programs that may not be as effective or efficient as those designed by anti-fraud experts.

§__.90(d)(2) Identity Theft Prevention and Mitigation

Once an institution has policies and procedures to identify risks of identity theft, it must also have reasonable policies and procedures to "prevent and mitigate identity theft in connection with the opening of an account or any existing account." We believe that this is generally an appropriate objective. Once the Agencies establish the objective, however, they should not then describe the process by which an institution is required to achieve it. The Proposed Rule states that an institution must: (i) obtain identifying information about, and verify the identity of, a person opening an account; (ii) detect Red Flags; (iii) assess whether the Red Flags evidence a risk of identity theft; and (iv) address the risk of identity theft. These requirements are too rigid and are unnecessary to achieve the stated goals. We believe that it would be more appropriate to require a financial institution to form a reasonable belief that the underlying transaction is legitimate (i.e., not the result of identity theft or account fraud) without requiring the institution to identify, assess and address every Red Flag. A financial institution need not identify every Red Flag that could apply in a given circumstance. Rather, any Red Flags identified in connection with their risk-based Program should be given appropriate consideration when determining whether or not the transaction is valid.

§ __.90(d)(2)(iii) requires that financial institutions assess whether the Red Flags "evidence a risk of identity theft" and states that "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 that this sentence be deleted. Mandatory review and analysis of each and every Red Flag will require creation of an entire department dedicated to the project. It is unnecessary and a waste of valuable resources for financial institutions to divert resources to such a time-consuming administrative exercise focused on reviewing and documenting and re-reviewing and re-documenting the same analysis. Financial institutions already have sufficient incentives to develop, implement, and refine identity theft and fraud prevention programs, as they generally suffer any financial loss and must contend with potential customer relations and public relations fall-out.

The Program must include policies and procedures to verify the identity of a person opening an account. Reliance on a Customer Identification Program ("CIP") as required under The USA PATRIOT ACT (the "CIP Rules") should constitute compliance with the Final Rule in connection with account openings. We also believe it would be appropriate for the Agencies to opine about the applicability of a Program to an account that is acquired through an acquisition, merger, purchase of assets or assumption of liabilities. These accounts are exempt from the CIP Rules because they do not fall under the definition of "account" under the CIP Rules. It makes sense for the Agencies to take the same approach in the requirements for the Program, since the risk to be mitigated for identity theft is best addressed at account opening. We request that the Agencies provide similar guidance in connection with the Final Rule. To do otherwise would not comply with the statutory requirement to be consistent with the CIP Rules.

§___.90(d)(5) Involvement of Board of Directors and Senior Management

The Proposed Rule states that a financial institution's Board of Directors must approve the Program. Although this is similar to the requirement imposed on a Board in the Information

Security Guidelines, we do not believe it is appropriate in this circumstance. It is not necessarily appropriate for the Board to consider the minutiae of a financial institution's fraud prevention efforts. Rather, this is a task more appropriately delegated to senior management with the relevant expertise. We also note that the actual operation of the Program will require adjustments on a continuous basis, and requiring Board involvement with these adjustments would be impractical and would hinder the institution's ability to modify its Program quickly to keep up with new methods of fraud and identity theft.

§ ___.82 Duties of Users Regarding Address Discrepancies

§ 605(h)(2)(A) of the FCRA requires the Agencies to issue regulations providing guidance regarding reasonable policies and procedures that a User should employ when the User has received a notice of discrepancy under § 605(h)(1). Congress specified that such regulations shall describe policies and procedures designed to: (i) form a reasonable belief that the User knows the identity of the person to whom the consumer report pertains; and (ii) "reconcile" the address with the consumer reporting agency by furnishing such address in the next regular furnishing cycle.

In general, Chase believes that the Agencies have proposed regulations that are consistent with the statutory requirement to form a reasonable belief that it knows the identity of the consumer in response to a notice of address discrepancy. Specifically, under § __.82(c) of the Proposed Rule, a User must develop reasonable policies and procedures to verify the consumer's identity if the User receives a notice of address discrepancy. The Agencies provide that a User that complies with the CIP Rules satisfies the requirement, regardless of whether the User is actually subject to the CIP Rules. We applaud the Agencies for including this clarification, and we urge the Agencies to retain it in the Final Rule. The statutory language in § 605(h)(2)(B)(i) is almost verbatim from the CIP Rules, and we assume Congress intended for the Agencies to implement the requirement in a similar fashion.

The statute requires that a User who receives a notice of address discrepancy must "reconcile" the address with the consumer reporting agency when a User "establishes a continuing relationship with the consumer." The Proposed Rule, however, expands this obligation on a User if it "[e]stablishes *or maintains* a continuing relationship with the consumer." (Emphasis added.) We urge the Agencies to eliminate the additional requirement not found in the statute. The level of regulatory burden imposed by this requirement is significant as it would force Users to reconcile and verify addresses millions of times a year in connection with routine account maintenance. The difficulty in verifying addresses would result in enormous costs that provide relatively little benefit to consumers. Additionally, under many state laws, creditors can only use an address provided by a consumer to send the consumer legally required notices (such as notices required before a motor vehicle can be repossessed). If the creditor is required to change the consumer's address on its records without the consumer's consent, the creditor will have difficulty providing legally valid notices under these laws.

Chase also requests that the Agencies delete the requirement in § __.82(d) that a User confirm the address of the consumer. As a threshold matter, the primary goal of § 605(h) of the FCRA is to prevent identity theft. The Agencies have proposed requirements designed to achieve

that goal, namely the obligation to form a reasonable belief that the User knows the identity of the consumer. Once the consumer's identity has been confirmed, it is not clear what congressional policy objective is achieved by going so far as to confirm the address itself. We also note that Congress appeared to specify what Users should verify (i.e., the consumer's identity) and how it should reconcile the address (i.e., by furnishing the address in question to the bureau if it establishes a continuing relationship with the consumer). With respect to the former requirement, it achieves the goal of preventing identity theft. With respect to the latter requirement, it precludes future Users from receiving the same notice of discrepancy and having to engage in additional diligence unnecessarily. Confirming the address itself does not appear to be one of the items Congress intended to require.

We also note that, as described above, the requirement in § 605(h)(2)(B)(i) is very similar to the requirement in the CIP Rules. By using the same language it would appear that Congress had intended for the Agencies to implement the requirement in a manner similar to that in the CIP Regulations. The Agencies have specifically opined that, under the CIP Regulations, an institution need not verify any particular piece of information collected, including the address. It is therefore likely that Congress did not intend for Users to verify the address.

There are also practical considerations that arise as a result of the requirement in the Proposed Rule to verify an address. For example, it is not clear how a User should reliably verify the address. It may be that trusted third parties do not have the address on file. It may also be that the User does not have evidence of the address change elsewhere in its files or among its affiliates' information. Reliance on the "consumer" is also not particularly beneficial, since the "consumer" may be the identity thief that provided the bogus information in the first place. Even if the address could be confirmed, § __.82(d) would impose significant costs on Users with little corresponding benefit in light of the fact that the consumer's identity had already been verified prior to confirming the address. It is also unclear how a User can comply with the statutory requirement to furnish the address as part of the next regular furnishing cycle if the address is not yet confirmed. Had Congress or interested observers understood § 605(h) to require address reconciliation, we believe this issue would have been clarified in the statute.

§ ___.91 Duties of Card Issuers Regarding Changes of Address

§ 615(e)(1)(C) of the FCRA directs the Agencies to prescribe regulations applicable to card issuers to ensure that if a card issuer receives a request for a new or replacement card within a short period of time after having received a notification of a change of address, the card issuer must verify the validity of the change of address.

The Proposed Rule would impose obligations on card issuers if they receive a notification of a change of address and then receive a request for a new or replacement card within a short period of time. The Final Rule should clarify that the obligations apply only if the creditor actually changed the address. The risk of identity theft occurs only if the address is changed as a result of such notification.

The Final Rule should provide that financial institutions comply with this provision if they verify the address at the time of the address change request or the time of issuance of a new card, whether or not the address change and the new card request are linked. Most financial 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 Final Rule allow broad leeway in the methods used by 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. The Final Rule 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 is one method recognized under the CIP Rules.

JPMorgan Chase & Co. appreciates the opportunity to comment on the Proposed Rule. If you would like to discuss any of our comments in more detail, please contact Andrea J. Beggs at 312-732-5345.

Very truly yours,

Andrea J. Beggs
Senior Vice President

JPMorgan Chase & Co. • IL1-0290, 1 Chase Tower, Chicago, IL 60670
Telephone: 312-732-5345 • Facsimile: 312-732-3596
andrea.beggs@chase.com