THE FINANCIAL SERVICES ROUNDTABLE

BITS

FINANCIAL SERVICES
ROUNDTABLE

September 18, 2006

To: Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, Office of the Comptroller of the Currency, Office of Thrift Supervision, National Credit Union Administration, and Federal Trade Commission

Re: Identity Theft Red Flags Proposed Rule

Dear Sirs and Madams:

The Financial Services Roundtable and BITS appreciate the opportunity to comment on the proposed "Red Flags Rule" which was published in the Federal Register on July 18. The proposal implements sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). Our member financial institutions applaud the Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, National Credit Union Administration, and the Federal Trade Commission (otherwise referred to as "the Agencies") for their work in this important area. As the Agencies well know, financial institutions have always been a favorite target for perpetrators of fraud and identity theft. Financial institutions have long answered this challenge with reliable business controls, advanced technology, knowledge sharing, and cooperative efforts with government and law enforcement agencies.

According to the proposal, the Agencies are jointly proposing guidelines for financial institutions and creditors in identifying patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The purpose of this letter is to provide the Agencies with comments on the proposed rule, including specific comments on nineteen of the thirty-one proposed red flags which are outlined in Appendix A.

Summary of Comments

The Roundtable and BITS strongly urge the Agencies to:

- Provide greater flexibility and explicitly state that the thirty-one red flags (and any others) be regarded as "examples" only;
- Clarify that the final rule should not be the basis for civil liability;
- Make the final rule more consistent with other regulations;
- Incorporate more realistic cost estimates of the impact of the regulation;
- Modify several key definitions; and
- Provide adequate time to implement a risk-based red flags program.

Greater Flexibility
Our members urge the Agencies to clarify in the final rule that the proposed thirty-one red flags should be viewed as "examples only," not as static requirements. A risk-based approach, as opposed to a static list of requirements, is essential and has worked well with the Agencies' Gramm-Leach-Bliley Act (GLBA) Information Security Safeguards Rule. Identity theft risks vary considerably based on many different factors including the nature of the product, origination/transaction channel, customer, size of institution, etc. An institution should consider each red flag during its risk assessment but only include those red flags in its program that are appropriate in light of its risk assessment.

A final Red Flags Rule should not be prescriptive in light of the fact that fraudsters constantly change tactics and financial institutions need the flexibility to respond to these changes. A set list of red flags today may not be relevant several years, even several months, from now as fraudsters develop new tactics. The rules should clarify that each financial institution has the flexibility to change its identity theft prevention program immediately and update it as the institution deems appropriate.

Our members are concerned that they will be placed in a situation where financial institutions must "prove a negative" and engage in unproductive negotiations with examiners and other government officials about why they chose not to apply one or more of the red flags. A financial institution should be permitted to incorporate the red flags which it reasonably identifies as materially significant, taking into account other facts such as concomitant expenses. An institution should not have to prove why a particular red flag was not implemented.

While our members applaud the "risk-based" approach in the proposed rule, they note that there appears to be a conflict within the details of the rule. The proposed rule emphasizes a risk-based approach in which each financial institution would tailor its approach to meet its unique situation, an approach which our members support. In contradiction to this approach, the Agencies are proposing regulations with thirty-one specific red flags. Our members urge the Agencies to clearly state in the final rule that the thirty-one red flags are examples only, and that financial institutions are encouraged to review these and consider them as well as identify other red flags that become apparent as fraudsters adapt and develop new techniques. Further, our members urge the Agencies to clearly state that financial institutions may achieve compliance without implementing all thirty-one flags.

To strengthen the Agencies' risk-based approach, our members strongly urge the Agencies to recognize in the final rule the reality that large, complex financial institutions may have multiple lines of business with responsibility for managing fraud and implementing an identity theft prevention and response program. In addition, our members urge the Agencies to recognize the fact that large, complex financial institutions have numerous training programs. The proposed rule requires financial institutions to "train staff to implement the program." Depending on the size and complexity of a financial institution, there can be training programs occurring in multiple lines of business. The rules also should clarify that institutions should, in three party transactions where they do not directly interact with the consumer, be permitted to rely on the originating creditor's compliance with this rule. We believe that failure to so clarify the rule will adversely impact the secondary market for assigned contracts.

Regarding section xx.82(d)(2), our members indicate that the verification sources listed are good, but that the proposed regulation should add account criteria under reasonable means. For example, if a Credit Reporting Agency (CRA) advises the financial institution of an address mismatch on an account that has not been active in the last six to twelve plus months, then the financial institution should not be required to expend resources to verify the new address. The Agencies should require that address change alerts delivered from the CRAs on existing accounts be noted by the users, along with the date of the alert. When the next high-risk transaction after that date (*e.g.*, security password change) occurs, the financial institution should verify the address prior to completing the transaction (if the alert was provided within the last six to twelve months).

Our members also note that portions of the proposed rule reach further than the statute contemplated, as evinced by committee reports and legislative history. For example, the proposed rules appear to require financial institutions to police identity theft in a manner contrary to legislative intent. Moreover, the Agencies have included business accounts whereas the statute addresses only consumer accounts.

Civil Liability Protection

The proposed regulation expands on the role of the financial institution and its customers. Traditionally, in banking, this relationship has been one of debtor and creditor. The regulation, as written, could impose upon the bank fiduciary obligations to actively prevent and investigate identity theft. Furthermore, the proposed regulation does not acknowledge that the best defense against identity theft is the customer himself/herself. The proposed regulation does not require the customer to participate in identity theft prevention. It imposes responsibility on banks to respond to certain factors which may suggest identity theft in circumstances in which the customer may already be aware and has chosen not to act. Our members urge the Agencies to clarify this issue in the final rule. We believe that financial institutions and creditors that have made a good faith effort to implement programs that are in accord with the rule should be protected from civil liability.

Greater Consistency with Other Regulations

Our members urge the Agencies to revise the rule so that it is more consistent with other regulations, specifically the GLBA Information Security Safeguards Rule and the USA PATRIOT Act's Customer Identification Program (CIP). The proposed Red Flags Rule is much more prescriptive than the GLBA information security guidelines rule, which our members believe strikes the appropriate balance. Our members believe the Agencies should adopt an approach similar to GLBA in the final Red Flags Rule.

With regard to the risk evaluation process, it is important to note that the proposed rule states factors that are nearly identical to factors that are already in place when opening new accounts. These factors are in place in accordance with the outlined procedures within the CIP rules issued to implement section 326 of the USA PATRIOT Act. The Agencies note that the CIP rules exclude a variety of entities from the definition of a "customer" and exclude a number of products and relationships from the definition of "account." For example, the CIP rules do not require customer identity programs for employee benefit plans or when a financial institution purchases a portfolio of assets. The Agencies do not propose any exclusion from either of these terms given the risk-based nature of the Red Flags Rule.

The CIP provides numerous procedures that help to protect the consumer. These regulations currently are sufficient. Our members encourage the Agencies to consider modeling the Red Flags Rule after the CIP guidelines to maintain a level of consistency.

The proposed regulations also are inconsistent with Section 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA 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. Our members note that it is important to ensure that any obligations to reconcile address discrepancies in the Red Flags Rule be consistent with any obligations that may arise under the USA PATRIOT Act Customer Identification Program.

Regarding section xx.82(c), duties of users regarding address discrepancies, our members noted this section creates a duty for users to verify the identity of the consumer for whom it has obtained a consumer report and receives a notice of address discrepancy even in cases where the user does not establish a relationship with the consumer. We would request clarification that in cases where a relationship is not established (i.e., an account is not opened) users are not required to verify the identity of the consumer, or, conversely, that verification is only required when the user establishes a relationship with the consumer. Our members dispute the need to engage in significant and burdensome verification for an applicant with whom a financial institution will not have a relationship. Also our understanding is that Congress intended to minimize additional regulatory burden by limiting requirements to instances where an account is established.

Regarding section xx.82(d)(3), our members request that the Agencies modify the definition of timing so that it should be "reasonable" timing. It would be burdensome and unreasonable for financial institutions to report each address change on the day it occurs. Financial institutions should report the address changes to the CRAs in the next monthly credit bureau reporting cycle.

Modifications to the Definitions

Our members urge the Agencies to modify several definitions for identity theft, customer, account, board of directors, red flags, and service provider.

Identity Theft. The proposed definition of identity theft is too broad and adds to public confusion over fraud *versus* identity theft. The proposed rule states "[t]he risks of identity theft to a customer may include 'financial, reputation and litigation risks that occur when another person uses a customer account fraudulently, such as by using the customer credit card number to make unauthorized purchases." By defining identity theft as using customer credit card numbers to make unauthorized purchases, the proposed regulation confuses fraud (lost, stolen, counterfeit cards/numbers) with true identity theft. Roundtable and BITS members urge the Agencies to consider applying the definition of "financial identity theft" that the BITS Identity Theft Working Group and BITS Fraud Reduction Steering Committee developed.

> "Identity theft" is the unlawful act of capturing, transferring and/or using one or more pieces of another person's personal identifying information (including, but not limited to name, address, driver's license, date of birth, Social Security number, account information, account login credentials, or family identifiers) and using or attempting to use that

information to establish or take over a credit, deposit, or other financial account ("account") in that person's name. Identity theft falls into one of two categories:

> **True name fraud:** Establishing (or attempting to establish) an account(s) using another person's identity.
> **Account takeover:** Establishing (or attempting to establish) control of an existing account(s) without authority of the account holder. Account takeover does not include solely the posting of unauthorized transactions against an existing account, such as, forged maker signature, counterfeit, credit card misuse.

Identity theft does not include identity manipulation/fraud, which is creating a fictitious identity using fictitious data combined with real information from multiple individuals, and then using this fictitious identity to establish (or attempt to establish) an account(s).

Customer. The proposed definition of "customer" encompasses both customer and account holders. Thus, "customer" means a person that has an account with a financial institution or creditor. Our members request that the Agencies clarify the scope of this term so that it is clear whether it applies only to natural persons or small businesses and other legal entities such as trusts, estates, or any incorporated or unincorporated organizations, including without limitation, corporations, partnerships or limited liability companies. Our members request that the definition be narrowed to mean a natural person, using credit or establishing deposit accounts for personal, family, or household purposes. Our members note that almost every other customer compliance and privacy regulation covers only natural persons and the FCRA does not reference business accounts.

Account. The proposed rule defines account as, "The various relationships that an account holder or customer may have with a financial institution or creditor that may become subject to identity theft." The Agencies requested comment on whether financial institutions and creditors should notify a customer when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years. Our members believe that if the account has been inactive that long, it implies a lack of interest on the part of the customer using this account and thus the financial institution/creditor should not be responsible for this notification. Moreover, the proposed term "inactive" is too broad and should be re-defined. A member provided an example that, while an account may not have activity such as purchases, advances, etc., the customer may still make payments on an account. While some Roundtable and BITS members note that the time frame of inactivity should be decreased to one year from two years, others note that this should be left up to the institution to decide, based on the risk, dollar amount and other factors. One member company suggests that the agencies tie the determination of whether an account is inactive to the time period required under escheat laws. While the time periods vary from state to state, banks are already set up to send notices of inactivity for escheat purposes. Having a different period for determining inactivity for escheat and identity theft purposes would be a significant burden and is likely to cause confusion.

The Agencies also request comment on whether the definition of an account should include relationships that are not continuing. Our members believe that the definition should exclude relationships that are not continuing or on-going with a financial institution or creditor.

Board of Directors: The Agencies use an expanded definition to address the fact that some institutions do not have an actual board of directors. The definition was expanded to include, in the case of a foreign bank or agency of a foreign bank, the managing official in charge of the branch or agency. A designated employee may be defined as the "board of directors" when any other creditor does not have a formal board. Our members believe financial institutions should be able to designate the appropriate official(s) to oversee the identity theft risk as with other compliance and risk-related programs. Moreover, section 114 of FACTA does not include a specific requirement that an institution's red flags program be approved by the Board of Directors.

Red Flags. The Agencies have defined "red flags" to include precursors to identity theft that indicate a "possible" risk. Our members urge the Agencies to modify the definition to either "probable" risk or "substantial risk" of identity theft. In light of the fact that almost anything is possible, a truly risk-based approach should be tied to probable risk or substantial risk of identity theft. Further, our members strongly object to the use of phishing as an example. While fraudsters use phishing to lure unsuspecting consumers, a phishing attempt by itself is not a precursor to identity theft unless the customer responds to the phish and supplies his or her credentials. Hence, our members urge the Agencies to modify the example to clarify that it is only a red flag when the customer, a service provider, law enforcement, or other third party notifies the financial institution that the customer has provided his or her credentials to a phisher/fraudster or when there is other unusual activity on the account.

Service Provider. The proposed definition of service provider is a "person or entity that provides service directly to the financial institution or creditor." BITS members urge the Agencies to change the definition to "a person, business or entity that provides a service directly to the financial institution or creditor." Also, it should be clarified that a service provider may implement its own program and need not necessarily implement the same procedures as the institution or creditor to whom it provides services.

Cost of Compliance

As required by the Paperwork Reduction Act of 1995, the Agencies have estimated the additional cost of compliance burden for the Red Flags program (knowing that this builds on existing requirements from the GLBA Security Standards and the CIP). The consensus of our members is that these estimates are extremely low and unrealistic. Some members suggest that the actual costs would be ten times greater than the estimates. In particular, large and complex financial institutions may have identity theft processes and programs in multiple lines of business which means the total estimated time to comply would be much higher. In addition, the estimated cost of compliance fails to consider the cost to third party service providers, neither creditors nor financial institutions, which may be required to implement a program.

Implementation Date

Our members urge the Agencies to provide adequate time for financial institutions and creditors to prepare and implement their programs. Full implementation will require numerous and significant changes to information systems as well as training programs. Our members propose that financial institutions and creditors be given 18 to 24 months from the date of the issuance of the final rule to comply with the rule.

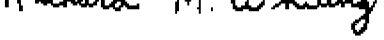
Conclusion

While the Roundtable and BITS applaud the Agencies efforts to increase protection of consumers from identity theft through their proposed Red Flags Rule, we urge the agencies to provide greater flexibility and explicitly state that the thirty-one red flags (and any others) be regarded as "examples" only; clarify that the final rule should not be the basis for civil liability; make the final rule more consistent with other regulations; incorporate more realistic cost estimates of the impact of the regulation; modify several key definitions; and provide adequate time to implement a risk-based red flags program.

Please see Appendix B for a brief overview of The Roundtable and BITS and our efforts to address identity theft and other information security challenges. If you have any further questions or comments on this matter, please do not hesitate to contact us or John Carlson, Senior Director of BITS, at john@fsround.org or 202.589.2442.

Sincerely,

Catherine A. Allen
CEO, BITS



Richard M. Whiting
Executive Director and General Counsel
The Financial Services Roundtable

Appendix A: Detailed Comments on the Thirty-One Red Flags
Appendix B: About the Roundtable and BITS

APPENDIX A: DETAILED COMMENTS ON THE THIRTY-ONE RED FLAGS

The following are comments from BITS/Roundtable members on some of the thirty-one red flags contained in "Appendix J" of the proposed Red Flags Rule. These comments are offered with the stated intent that the Agencies treat the red flags as examples, not requirements. Some of our members question the helpfulness of some of the red flags in the proposed rule. Although financial institutions are willing to devote resources to mitigate identity theft, it is important to identify effective and efficient procedures.

Information from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

Comment: There are many reporting agencies on the market and financial institutions have numerous means of being provided with this required information. Our members request that this red flag include "other service provider" (other than a CRA) as there are clearing services that will advise of fraudulent Social Security Numbers, addresses, etc.

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

Comment: When collecting a great deal of information from clients, misprint errors are a common cause of address discrepancies. Due to this factor, our members request that this red flag be modified to include only true and substantial address discrepancies[1] and not misprint errors. In addition, our members request that a safe harbor be added to this red flag to protect against private rights of action for "negligent compliance," and that this safe harbor be applied whether or not the notice of address discrepancy is used as a red flag by the financial institution (i.e., is applied to § --.82(d) as well). Because some financial institutions already over-report address discrepancies, to ensure compliance with the FCRA, our members urge careful and clear guidelines to increase the efficiency and efficacy of such reporting. Address discrepancy requirements also are likely to generate false positives due to the large number of consumers each year who move.[2] Our members also believe that open-ended and revolving credit arrangements are at much greater risk in cases of address discrepancy than are closed-ended credit arrangements. Mortgages and similar closed-ended arrangements should be expressly excluded from this red flag.

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:*

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

Comment: The phrase "activity that is inconsistent with history" is very vague. Depending on how a financial institution or regulatory interprets this, it may not be an

[1] One creditor reported that on a recent request for over four and a half million credit reports, it experienced an address match rate of ninety-two percent. This would potentially require address reconciliation on over 360,000 accounts. This reconciliation requires significant human and systems resources with a very limited potential benefit.

[2] The United States Postal Service reported that, in 1998, approximately seventeen percent of the United States' population moved. That year, the Postal Service processed forty-four million change of address requests.

indication of identity theft. The Agencies should be more specific about this red flag or remove it. Moreover, a member noted that this information may not be available from credit bureaus.

.

Documentary Identification

4. Documents provided for identification appear to have been altered.

Comment: In numerous situations, not only is altering an indication of identity theft, but it is also forgery. Our members encourage the Agencies to add forgery as a part of this red flag. Moreover, our members urge the regulators to provide tools to help financial institutions detect fake identification or fraudulent credentials. Altered documents are often very difficult to identify. This is one reason why our members are increasingly concerned about the authenticity of credentials issued by state and federal government agencies.

Personal Information

8. Personal information provided is inconsistent when compared against external information sources. *For example:*

- **a.** The address does not match any address in the consumer report; or
- **b.** The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

Comment: Misprints and typographical errors are a common discrepancy with this red flag. Therefore, our members urge the Agencies to distinguish between inconsistencies due to fraud vs. the inaccuracy of information and/or data due to error (e.g., typo, inquiry error). This proposed red flag (in addition to 10, 12 and 14) raises the issue of whether a financial institution is expected to compare information submitted with information on file just within a specific line of business or across the entire enterprise. For example, it may be a simple matter for a banker making a credit card application in a one-branch bank to compare the signature on the application to that on a DDA signature card; but it is a far different matter for large financial institutions with thousands of branches.

9. Personal information provided is internally inconsistent. *For example*, there is a lack of correlation between the SSN range and date of birth.

Comment: The Agencies should clarify what "internally inconsistent" means and insert "when compared against external information sources" at the end of the sentence. Further, this could be very costly for financial institutions to validate, given that there is not a means for financial institutions to directly validate Social Security Administration Data (and a reason why BITS and its members have been urging the SSA to develop a consent-based verification program). The Agencies also should clarify whether a financial institution's Customer Information Program (as required under section 326 of the USA Patriot Act) is sufficient.

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.

Comment: Several financial institutions noted that they take applications from many different sources and very few financial institutions consolidate them into a single source. Building such a database would be costly with a questionable return on investment. Our members suggest that the Agencies remove this red flag. If the agencies decide to retain this red flag, our members urge the Agencies to clearly define "known" in this red flag as "known to the financial institution" so that information known, for example, to law enforcement is not included.

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.

Comment: There may not be reliable ways for identifying phones associated with pagers or answering services.

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.

Comment: This information (with the exception of the SSN) changes so often that it is hard to include such a prescriptive red flag/example. Our members urge the Agencies to remove the use of the address and phone numbers as identifiers from this red flag. This red flag should not require a financial institution to develop systems and databases that are not already in existence. Further, an exception is needed for related customers who may share addresses or phone numbers. Finally, some financial institutions may not have a file that includes all customers across lines of business.

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

Comment: There are numerous occasions where this occurs (e.g., when a customer moves, lack of customer focus in response to a death in the family). Many of these occurrences are not identity theft and therefore should not be a red flag. Our members encourage the Agencies to strike this from the list of 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.

Comment: Because financial institutions generally do not have access to information beyond that which is found in a wallet or consumer report, our members urge the Agencies to make clear that financial institutions are not required to request, obtain, or verify information that would not be available from a wallet or consumer report.

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 cell phone, or for the addition of authorized users on the account.

Comment: Many institutions do not have links between change of address requests and requests for new or additional cards or checks, although these institutions do verify the identity of consumers requesting the change of address or the new cards or checks. Our members urge clarification that Section xx.91(c)(3), which permits an institution to use other means of assessing the validity of a change of address, is satisfied where the institution has reasonable procedures to validate the legitimacy of the request when the request is made, regardless whether requests are made thereafter for new or additional cards. Further, one member pointed out that a request for new checks in close proximity to a check order is not necessarily an indicator of ID theft and may be a normal, legitimate customer driven activity.

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

Comment: This is a common occurrence as customers forget to send a change of address. Consequently, this is too broad to be a useful red flag. Our members encourage the Agencies to narrow this red flag to product lines, such as home equity accounts, where undeliverable mail is more likely to evince fraud.

Anomalous Use of the Account

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

For example:

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

Comment: This is not an acceptable indication of identity theft as credit default is not necessarily identity theft. Our members encourage the Agencies to remove this from the list of red flags.

20. An account that has been inactive for a reasonably lengthy period of time is used. (Taking into consideration the type of account, the expected pattern of usage and other relevant factors.)

Comment: The term "inactive" can have varying definitions across financial institutions. Our members urge the Agencies to grant financial institutions the flexibility to conduct their own risk assessment to determine when an account is deemed "inactive" and when this poses a risk of identity theft.

Notice from Customers or Others Regarding Customer Accounts

21. The financial institution or creditor is notified of unauthorized charges that are in connection with a customer's account.

Comment: The use of unauthorized charges is too broad and not specific to identity theft. Therefore the financial institutions urge the Agencies to include the term "identity theft-related" to the statement.

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

Comment: This may not necessarily be an indication of identity theft. For instance, it is common for customers to forget to report a change of address. Furthermore, many customers choose not to receive statements via the mail, but access them on-line. At a minimum, the Agencies need to state that many customers do not receive statements via postal mail anymore.

25. Electronic messages are returned to mail servers of the financial institution or creditor that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to the website of the financial institution or creditor.

Comment: Fraudsters send thousands of phishing emails daily. A phishing attempt rarely results in identity theft. It may occur only when a customer responds to a phishing attempt and supplies credentials to the phisher/fraudster. Thus, the red flag should be changed to state that it is only a red flag when the customer, a service provider, law enforcement, or other third party notifies the financial institution that the customer has provided his or her credentials to a phisher/fraudster or when there is other unusual activity on the account.

Other Red Flags

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

Comment: This is not a sufficient indicator of identity theft. Also, it is not clear what steps the Agencies expect financial institutions to take when this does occur. Our members urge the Agencies to clarify.

Some members recommend including an additional "example" of an important red flag: failed verification on existing account holders in an attempt to access their account. The rationale is that if someone fails this verification, it should then serve as a red flag.

APPENDIX B: ABOUT THE ROUNDTABLE AND BITS

The Financial Services Roundtable is a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Roundtable member companies provide fuel for America's economic engine, accounting directly for $50.5 trillion in managed assets, $1.1 trillion in revenue, and 2.4 million jobs.

BITS is a nonprofit industry consortium that shares its membership with The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. By sharing information, developing and disseminating guidelines and successful strategies, and fostering open dialogue, BITS members have helped to decrease the risks associated with fraud and identity theft. Where identity theft does occur, BITS members are proactive. BITS and the Roundtable, with fifty of our member institutions, co-founded the Identity Theft Assistance Center (ITAC) in 2004. As of July 2006, the ITAC has helped over 6,000 individuals to restore their financial identity. These services are provided free to consumers by ITAC members.

Within BITS there are two working groups that have a strong interest in the Red Flags regulation—the information security experts who are involved in the BITS Security and Risk Assessment (SRA) Working Group and the fraud reduction experts who are involved in the BITS Fraud Reduction Steering Committee (FRSC). The mission of the SRA is to strengthen the security and resiliency of financial services by sharing and developing best practices to secure infrastructures, products and services; maintaining continued public and private sector confidence; and providing industry input to government agencies and regulators on policies and regulations. The mission of the FRSC is to identify fraudulent trend activity, reduce fraud losses, and foster new opportunities to reduce the impact of fraud on the financial services industry and our customers. Participants in the BITS Fraud Reduction Steering Committee include representatives from financial institutions, industry associations and the Federal Reserve.

Much of BITS' work is published for the entire financial services industry to use in efforts to combat fraud and tackle identity theft. Please see the BITS web site to access public documents on efforts to address fraud, identity theft, and a range of relevant security-related issues: http://www.bitsinfo.org/p_publications.html.

###