September 18, 2006

Federal Trade Commission/Office of Secretary
Room 159-H (Annex C)
600 Pennsylvania Avenue N.W.
Washington, DC 20580

Subject: The Red Flag Rules, Project No. R611019

Dear Sir or Madam:

Boeing Employees' Credit Union (BECU) appreciates the opportunity to provide comments on the proposed Red Flag Rules stemming from the Fair and Accurate Transaction Act of 2003 (FACTA). BECU is a state-chartered, federally insured credit union with assets of $6.6 billion and a membership base of over 455,000.

Here are our responses to your questions:

1. Red flags are generally defined as patterns, practices, or activities that indicate the possible risk of ID theft. This would include situations in which there is a "possible" risk of ID theft, even though the existence of ID theft is not necessarily indicated, such as the receipt of a "phishing" email or security breach. Should the definition of "red flags" include these possible risks of ID theft?

At our credit union, if a member contacts us that they have been "phished", we feel the attempt has been unsuccessful due to their acknowledgement and the steps we have to secure access to their account(s). We don't feel that a receipt of a "phishing" email should trigger a red flag because it would lessen the impact of red flags for more likely instances of identity theft. Most of the population receives phishing emails; however, few are then subject to identity theft unless of course the person falls for the scam. At which point we already have steps to secure the members' accounts. If there is a security breach on the part of BECU or any of our vendors, we feel the Red Flag makes sense. We know that there is a potential exposure on a specific account(s) and follow our state and the NCUA requirements to contact the affected members and our regulator.

2. The Program must include relevant "red flags" from: 1) Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation that is included as Appendix A to the proposed rules; 2) any applicable supervisory guidance, either now or in the future; 3) incidents of identity theft that financial institutions have experienced; and 4) methods of identity theft financial institutions has identified that reflect changes in identity theft risks. Are these appropriate sources?

Yes, we feel this is a complete list and cannot think of any others to include.

3. A financial institution using a third party's computer-based programs to detect identity theft must independently assess whether the programs meet the requirements of these rules and should not rely on the representations of the third party. What impact will this have on the policies and procedures that you currently have to detect and mitigate identity theft, including on third party computer-based products that you currently use?

Our vendor review process will need to include a specific review of the proposed vendor's identity theft capabilities. The value-add of using a third party computer based program to detect identity theft is diminished

when you must independently verify the third party's compliance with the rules. This requirement makes it harder to comply. It adds expense to automating a process. The added expense will act as a disincentive to use computer based programs. Rather than obtaining added security through computer based programs, some will forego the expense and hassle associated with the "independent assessment" and continue to accept the risk without macro analysis assessment tools.

4. In identifying the relevant "red flags" for its program, the institution must consider which of its accounts are subject to the risk of identity theft; the methods it provides to open these accounts; the method it provides to access the accounts; and its size, location and member base. Are these factors appropriate and should any others be considered?

This seems to be a complete list. In our opinion, however, any account is potentially subject to identity theft. The regulators should be clearer or more specific on what ones they feel have a bigger potential for identity theft and ways they feel identity theft can be prevented.

5. The proposed rules include a number of actions that a financial institution may take to address the risk of identity theft, such as monitoring an account for evidence of identity theft; contacting the consumer; changing passwords, security codes, or other devices that permit access to an account; reopening an account with a new account number; not opening a new account; closing an existing account, notifying law enforcement, and possibly filing a Suspicious Activity Report; implementing any requirement for limiting credit extensions, such as declining to issue an additional card if there is a fraud or active duty alert on the credit report; and implementing any requirement that a furnisher of credit information to a credit bureau has for correcting or updating inaccurate information. Should these all be included as examples and are there any other appropriate examples?

These appear to be appropriate examples but we hope they are provided only as "suggestions" and not be required and allow the financial institution to determine the best method of protecting consumers' information.

6. Would it be appropriate to allow a service provider to implement a Program that may be different from the one developed by the financial institution? Is it necessary to address service provider arrangements in these rules or would it be self-evident that the institution would be responsible for complying with these rules, even if they contract with a service provider to perform these activities?

We feel financial institutions have the freedom of contract and may not choose to do business with a service provider who has a program that is not consistent with its own. We feel that service provider arrangements do not need to be addressed in these rules as all liability rests with the financial institution.

7. Will annual reports to the board, a board committee, or senior management regarding compliance with these rules be sufficient? Are the responsibilities allocated between the board and senior management regarding the required oversight and reporting of the Program sufficient?

Yes, we believe that annual reports to the board regarding compliance would be sufficient.

8. Are the "red flags" listed in the proposed guidelines, which will be outlined in the appendix to these rules, too specific or not specific enough? Should additional or different ones be included?

A couple of the red flag indicators cause us some concern: Under Address Changes, number 17 "Mail sent to the customer is returned as undeliverable although transactions continue to be conducted in connection with

the customer's account." We receive a lot of mail undeliverable. For us to have to go into each of these accounts to see if any recent activity has been done and if so, to ensure that the person performing the activity is the actual owner of the account would be overly burdensome. Also under the Anomalous Use of the Account, number 18 "The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronic equipment or jewelry)". Again, this would also be overly burdensome and we're not sure our members would like us questioning them on what they are using their credit cards on.

9. One of the "red-flags" listed is when an account is being used after being inactive for a long time. The FACT Act indicates that the account should be inactive for two years before it should be considered a concern. Should the rules include the two-year time period or should a time period not be listed to take into consideration the different types and usage of various accounts?

In our opinion, financial institutions should determine time frames because different segments of customers and account types dictate usage patterns. Additionally, Uniformed Abandoned Property Laws already handle some of these timing issues to the extent that BECU, as a Washington State corporation escheat funds if no activity after three years.

10. When required to determine the validity of a request for an additional or replacement credit or debit card shortly after receiving a change of address request, the card issuer must either: 1) notify the cardholder of the request at the cardholder's former address and provide the cardholder with a means to promptly report an incorrect address; 2) notify the cardholder of the address change request by another means of communication previously agreed to by the issuer and cardholder; or 3) use other means of evaluating the validity of the address change. Is further elaboration needed regarding these means of verifying a change of address request?

Option 3 needs explanation. We need a better understanding of what actions are considered acceptable means of verifying a change of address as it relates to requests for additional or replacement credit or debit cards.

11. Any written notice to consumers regarding change of address discrepancies must be clear and conspicuous and separate from the regular correspondence to the cardholder. Should there be further elaboration regarding these notices?

Clarification on whether electronic notices would be acceptable if the cardholder has previously contracted for electronic communication from us.

12. The user of credit report information must use reasonable policies and procedures for verifying the identity of the consumer for whom it has obtained a credit report whenever the user receives a notice of address discrepancy from a credit bureau. Using the policies and procedures regarding identification and verification that are outlined in the CIP rules will satisfy this requirement. Are these CIP procedures sufficient?

Our Customer Identification Procedures address when an address on a credit report is different from what was provided by the applicant, we take necessary steps to identify that person. If the credit bureau lists a phone number to call to verify that person, that is what we do.

13. When certain conditions are satisfied, a user of credit information must use reasonable policies and procedures for furnishing to the credit bureau, from which it received a notice of an address discrepancy, the address for the consumer that the user has reasonably confirmed is accurate. Methods to do so include

verifying the address directly with the consumer, reviewing its own records of the address that was provided in requesting the credit report, verifying the address through third party sources, or using other reasonable means. Should these methods be included and are there other methods that should be included?

These methods seem sufficient.

14. For new relationships, the user of the credit information will furnish the address that it confirms as accurate to the credit bureau for the reporting period in which it establishes the relationship with the consumer. For other circumstances, such as when there is already an existing relationship with the consumer, the user should furnish the information for the reporting period in which the user confirms the accuracy of the address. Are these time periods appropriate?

They seem appropriate.

Thank you for the opportunity to respond to the proposal. We look forward to the final outcome.

Sincerely,

Gary J. Oakland
President and CEO

Joe Brancucci
Vice President of Product and Delivery Channel Management and Chief Lending Officer