From: Cheryl Nakashige [mailto:cnakashige@candcbank.com]
Sent: Friday, September 08, 2006 3:31 PM
To: Comments
Subject: Comment Letter RIN 3064-AD00

Mr. Robert E. Feldman, Executive Secretary
Attention: Comments
FDIC
550 17th Street NW
Washington, DC 20429

RE: Comment Letter to Identity Theft Red Flags and Address Discrepancies Under the FACT Act of 2003

Dear Mr. Feldman:

Thank you for the opportunity to comment regarding the above proposal. First and foremost, I am totally opposed to the burdensome nature of this proposal. The estimated burden to implement the regulations and guidelines is vastly understated at 25 hours to create the Program, 4 hours to prepare an annual report, and 2 hours to train staff (my estimate is to at least triple those figures). The estimated burden section goes on to state that "The Agencies believe that most of the covered entities already employ a variety of measures to detect and address identity theft that are required by section 114 of the proposed regulations because these are usual and customary to business practices that they engage in to minimize losses due to fraud." If that is the case (and it generally is), why then place additional identity theft burdens on financial institutions. Our bank has $850 million in assets and is staffed by only one compliance officer who is up to her eyeball's in trying to comply with all the existing laws and regulations, guidelines, Financial Institution Letters, etc. – not to mention implementing even MORE under the FACT Act and other proposals that are always looming in the background. Where is the regulatory reduction that is supposed to be occurring!! It's funny to note that a under the section where it states that a written identity theft program is required, footnote 19 states that "Agencies are expected to take into account the limited personnel and resources available to smaller institutions and craft such regulations and guidelines in a manner that does not unduly burden these smaller institutions." Maybe the regulatory agencies failed to see this small print since there is no mention in the proposed regulations that only institutions under $1 billion don't need to comply with particular sections. The way the proposal is written is that it will apply to every asset size institution, whether there in one part-time compliance officer or 2,000 compliance officers. It does not matter that the program must be appropriate for the size and complexity of the financial institution and the nature and scope of its activities since an enormous effort will need to be made to develop such programs and continually monitor.

Furthermore, why should financial institutions bear the brunt of having to detect identity theft when every consumer in our nation can get a free copy of their credit report from each of the three major credit bureaus for FREE. It should be the consumer's responsibility to review their credit reports, look at account statements, close out accounts if they are aware that identity theft may occur (i.e., someone stole their social security number), and the like – not the financial institution's responsibility!

The FACT Act required the regulatory agencies to:

(A) establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary; and
(B) prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to subparagraph (A), to identity possible risks to account holders or customers or to the safety and soundness of the institution or customers.

The guidelines cannot be inconsistent with the policies and procedures required under section 326 of the USA PATRIOT Act, which requires verification of the identity of persons opening new accounts. I firmly believe that with the comprehensive Customer Identification Programs (CIP) that are required at financial institutions, this should be sufficient since identity theft could be prevented at account opening. Financial institutions also are the one industry that has probably the strictest regulations in place for safeguarding customer information and do the best job at it. Once again, financial institutions are being the scapegoat to identify and protect identity theft victims just as we are the gatekeepers for identifying suspicious activity under the BSA. We are not provided any funding from the federal government for these efforts that consequently reduce financial institution's income and place additional burdens on customers and staff for complying with these government mandates.

Incorporating Red Flags shown in Appendix J, assessing the validity of change of address requests, and inactive account procedures all appear reasonable methods for inclusion in an institution's Identity Theft Program to minimize identity theft. The following are comments regarding certain sections of the proposal that I would like considered in the event that the proposal may be put into effect as is:

FDIC Section 334.82 Duties of users regarding address discrepancies.

- It states that a user who employs policies and procedures under the CIP satisfies the requirements for address discrepancies; however, the CIP regulation does not indicate that address discrepancies are a requirement. If an institution does not specifically have address discrepancies in written form in its CIP program, it is confusing as to whether a bank would then need to comply. This should be clarified.
- *I am opposed to requiring financial institutions to furnish a consumer's address to a consumer reporting agency when there is an address discrepancy*. Although our bank reports our customers' credit records to all three consumer reporting agencies, I don't believe this is a regulatory requirement. In essence, it appears that this new requirement for reporting accurate addresses to credit bureaus would now require financial institutions to begin reporting credit information if they had not done so previously. I don't know the process for uploading credit information to credit bureaus electronically or know whether addresses are specific fields that are required. If they are not, then I'm not sure how a regulatory agency can expect financial institutions to comply with this additional burden, especially if the credit information can only be sent electronically. If an address is a required field, then I would believe we already would be in compliance once a relationship is established and we report the current address of the customer. If a customer moves and changes address, it should not be the bank's responsibility either to report this new address to the credit bureaus *as a regulatory requirement*. Again, since I'm not familiar with credit information being furnished to credit bureaus, an address change may be ultimately reported if the institution has changed the address on its system and that particular field of information can then be electronically forwarded. Nevertheless, all these requirements are an additional burden on financial institutions that is not warranted.

FDIC Section 334.90 Duties regarding the detection, prevention, and mitigation of identity theft.

- Account definition section 334.90(b)(1) – this should not include relationships that are not "continuing." It should only apply to new or existing customers that have accounts at the institution and not consumers who may only be inquiring or pre-qualifying for a product or service (or that do not open an account).
- Identity Theft Prevention Program section 334.90(c)(2) – it states that the Program must be designed to address changing identity theft risks based on experience, changes in methods of identity theft, etc. Criminals are inventing new methods of committing identity theft every day, and I don't quite understand how a regulatory agency could require financial institutions to be fluent in knowing all identity theft risks. Does this mean every time a new type of fraud is discovered, that policies and procedures need to be updated. This could be a full-time job. *I am opposed to the burden that this requirement would put on financial institutions*.
- Development and implementation of Program section 334.90(d) – it states that at a minimum, the Program must incorporate any relevant Red Flags from Appendix J, supervisory guidance,

incidents of identity theft experienced, and changing of identity theft methods. The agencies would not define what is "relevant." Each of the red flags shown in Appendix J could be relevant since a financial institution does not know if or when one of the types of identity theft or precursors could occur and any type of account could be affected by identity theft at any point in time. It would be too burdensome to put a program into place that is only surmising the changes that occur in this area. In fact, the proposal states that "While the Agencies expect to update Appendix J periodically, it may be difficult to do so quickly enough to keep pace with rapidly evolving patterns of identity theft or as quickly as financial institutions and creditors experience new types of identity theft." Further, it states that "Given the changing nature of identity theft, a financial institution or creditor must incorporate Red Flags on a continuing basis so that its Program reflects changing identity theft risks to customers and to the financial institution or creditor as they arise." This sounds like every financial institution will now have to employ an "Identity Theft Officer" just as they do a privacy officer and a BSA officer and most likely purchase expensive software to detect fraud. *I totally oppose this section due to the burdensome nature and lack of financial and human resources to comply at most financial institutions.* We do not currently have any such fraud detection tools in place. Our bank's automated anti-money laundering software (purchased due to the onerous requirements of the BSA) only looks for suspicious activity and cannot make the determination that identity theft may have occurred on an account.

- Development and implementation of Program section 334.90(d)(2)(ii) – it is proposed that financial institutions have policies and procedures to detect red flags. *This is unduly burdensome, costly, and in some case, not feasible and I am opposed to this.* For example, #8b in Appendix J reveals a red flag as "the social security number has not been issued or is listed on the SSA's death master file." Since a financial institution is not able to validate the SSN given to the one issued by the SSA, how is a regulatory agency to expect that we follow this red flag. Financial institutions should have access to a secure database in order to validate SSNs with the SSA. This would probably prevent a majority of the identity theft when opening accounts. Other red flag examples are much too vague such as #3a (a recent and significant increase in volume of inquiries – may be credit shopping); #9 (personal information provided is internally consistent such as lack of correlation between the SSN range and date of birth – example is much too burdensome and cannot be accomplished efficiently without automation); #11a (address on an application is fictitious, a mail drop, or prison – too burdensome and cannot be accomplished efficiently without automation); #11b (phone number is invalid or is associated with a pager or answering service – pagers can be legitimate for businesses and how are we to know that a number is invalid); #14 (personal information provided is not consistent with information that is on file); a material change in the use of credit, especially with respect to recently established credit relationships – maybe a 20-year-old is opening his or her first new credit accounts); #19a (nonpayment when there is no history of late or missed payments – what is the customer just lost their job and couldn't make a payment); 19c (a material change in purchasing or spending patterns – going way overboard in making us monitor purchasing patterns of customers); 19e (a material change in telephone call patterns in connection with a deposit account – not feasible to monitor); and #21 (financial institution is notified of unauthorized charges in connection with a customer's account – are Regulation E unauthorized payment claims now considered identity theft cases as well).
- Staff training – *I am opposed to this being a regulatory requirement.* It may already be taking place at financial institutions but it is much too burdensome and costly to continually train staff in this area as a regulatory requirement. It should be encouraged but not required. There are very few regulations (maybe BSA and Regulation CC) that require training. Regulatory agencies don't need to begin adding this burden to any new regulations that come along.
- Oversight of service provider arrangements – *these do not need to be addressed in the regulation and should be removed* since regulated institutions must comply with other regulations or guidelines regarding service providers.
- Involvement of board of directors and senior management and Reports – *opposed to the Board or committee thereof needing to approve a written program and annual reports being provided*. Again, this is more burdensome regulation that is not necessary. The Boards of financial institutions are already inundated with BSA reporting, security reports, compliance reports, and all

the ordinary issues they address. The Identity Theft Officer (since one will now need to be appointed) also will not have the time to provide annual or more frequent reports. It is recommended that a written program be implemented but that Board approval is not required. Annual reports on this type of activity is not necessary and should be eliminated.

Duties of card issuers regarding changes of address.

- Form of notice – a model notice would be helpful so that a financial institution is not cited for the notice not being clear and conspicuous.

Final Thought – It took nearly all day to just complete this comment letter since I, as compliance officer, have been inundated with compliance requests from the staff. This occurs on a daily basis. And then regulatory agencies expect us to find the time to put together a written Identity Theft program addressing all the regulatory requirements!! Please give us financial institutions some relief from this massive overload of compliance requirements! Thank you for your consideration of these comments.

Sincerely,

Cheryl Nakashige, VP
Compliance Officer
Citrus & Chemical Bank
cnakashige@candcbank.com