From: "Kevin Mitchell" <KMitchell@peoplesbanktexas.com> on 09/11/2006 11:30:03 AM

Subject: Identity Theft Red Flags and Address Discrepancies

Ladies & Gentlemen,

I appreciate the opportunity to comment on the "Red Flags" proposal implementing Section 114 of the FACT Act.

I have several concerns about the proposal in general and about the overall tenor of the proposal. I have two main concerns with the proposal in general, and other concerns deal with how the proposal can be practically implemented.

1. The proposal is to implement the Fair CREDIT Reporting Act, as modified to include the Fair and Accurate CREDIT Transactions Act, and yet the proposal indicates in several places that the requirements will apply to Deposit accounts and that an institution might also apply the proposals to small business accounts. I believe this reach is beyond the intent of the Acts and beyond the intent of Congress in passing the Acts.

- In the summary the middle of page 12 addresses the scope of a bank's program for detecting and mitigating possible ID Theft risks. By stating that the bank must determine if the program will cover only credit accounts or if it will also include deposit accounts, the agencies have expanded the Fair and Accurate **Credit** Transactions Act and the Fair **Credit** Reporting Act, as amended to implement the FACT Act, to not just apply to consumer credit relationships but now also deposit products, and business products held by an individual. I believe this is beyond the intended reach of the acts and therefore is not specifically authorized by congress – to apply the acts to anything other than credit accounts as they relate to consumer reports and reporting.
- The middle of page 12. Addressing the scope of a bank's program for detecting and mitigating possible ID Theft risks. By stating that the bank must determine if the program will cover only individual customers or if it will include small businesses.

The very basis of the FCRA and the FACT Act is for consumer protection, and the FCRA discusses only "Consumer Reports". I believe the proposal expands the reach beyond the intent of the acts. This argument would also apply to the statement on the bottom of page 16 that indicates the agencies specifically did not pick a time period for defining when an account had been inactive for a "reasonably lengthy period of time" because of the variety of credit & deposit products covered. And to the statement on page 17 that indicates the proposal would cover a request by an individual for a business card.

2. I also feel there is an overall tenor in the proposal that leaves the reader with the impression that it is the duty of all financial institutions to protect individuals from identity theft, and that if someone becomes a victim of identity theft that the financial institution is at least partially, or fully to blame.

- In the summary the middle of page 10 there is a statement that banks are at litigation risk for failure to adequately protect customers from identity theft. I feel this would add legitimacy to any future court cases where ID Theft victims will sue the bank and claim is was the bank's fault, and seek damages, no matter how the identity theft occurred or even if how it occurred can not be determined. According to information in a recent seminar, Pulse EFT and the L.A. County Sheriff's office indicate that the top two ways that identity theft occurs are by employee theft (a waiter or office worker at a doctors office etc. records card information to sell on the black market) and through dumpster diving or a stolen wallet or purse. There have been few cases, if any where the identity was stolen from a financial institution.

I think the statement would have far less potential for misuse if it said

"… failure to adequately protect customer information that is retained by the bank ".

3. Another concern is how the requirements of identifying and responding to certain Red Flags can be carried out in the real world.
Appendix J lists the following Red Flags:

+ Address provided is the same as for a known fraudulent application
+ Phone # provided is the same as for a known fraudulent application
+ Personal information provided is associated with known fraudulent activity

Will this require that we have a database of known fraudulent applications that we can cross check against all new applications? We don't keep such a database.
Will it require Credit Reporting Agencies to create such a database, and / or require credit card servicing and transaction servicing companies (Certegy, etc) and/or Credit Reporting Agencies to create such a database, thereby increasing the cost for loan applicants?

+ Address is fictitious / a mail drop / a prison
+ Address / SS # / Phone # is the same as other applicants or customers

Will this require that we have a database of all prior applications (denied & approved) that we can cross check against all new applications?
We can search our main-frame system for address & SS # but we can not search by phone #.
How can financial institutions in larger cities and MSAs know all addresses that are mail drops?

+ Personal information is the type commonly associated with fraudulent activity

What personal information is <u>The Type</u> commonly associated with fraud?

4. Another general concern is that too much monitoring by lenders / card issuers; too much artificial intelligence software will restrict activity too tightly & therefore would stop legitimate customer activity. For example, I recently changed jobs and moved from one state to another. During the move I used a credit card to cover all my moving expenses, to buy new furniture, etc. and this card had been inactive for about two years. This was convenient and helped during the transition, however in my scenario I would have set off several Red Flags

A. New address
B. Phone # disconnected
C. No home phone # at new address
D. Using a card that was inactive for some time
E. Buying furniture, electronics, gasoline, and groceries with the card
F. Running up a large balance when there had not been one for 2+ years

I am sure that, if this proposal would have already been in place my card would have been shut down and I would have had a lot more hassle, on top of all the normal hassles of moving.

Thank you for the opportunity to comment and as you review the proposal for finalization please consider that the overall tenor of the existing proposal places too much responsibility for identity theft on financial institutions.

Kevin Mitchell, CRCM
Sr. V.P. Regulatory Compliance
Phone: (806) 794-0044
Fax: (806) 771-2268
Addr: 5820 82nd Lubbock, TX 79424
www.peoplesbanktexas.com