RILEY, CALDWELL, CORK & ALVIS
ATTORNEYS AT LAW
A PROFESSIONAL ASSOCIATION

FRANK A. RILEY
PAT CALDWELL
STEVEN E. CORK
LES ALVIS
J. DAVID HALL

OF COUNSEL:

E. LAKE TOLBERT
DAVID R. SPARKS

■ TUPELO OFFICE
207 COURT STREET
TUPELO, MISSISSIPPI 38804
POST OFFICE BOX 1836
TUPELO, MISSISSIPPI 38802-1836
(662) 842-8945
FAX (662) 842-9032

□ JACKSON OFFICE
525 EAST CAPITOL STREET, SUITE 405
BANCORPSOUTH BUILDING
POST OFFICE BOX 22491
JACKSON, MISSISSIPPI 39225-2491
(601) 352-2092
FAX (601) 352-2095

September 18, 2006

Jennifer J. Johnson, Secretary
Board of Governors of the Federal
Reserve System
20th Street and Constitution Ave., NW
Washington, DC 20551
regs.comments@federalreserve.gov

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429
Comments@FDIC.gov

Re: Comment on Behalf of BancorpSouth Bank
In Re Joint Proposal Rulemaking
Implementation of Sections 114 and 315
of the FACT Act
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 RIN 3084-AA94
71 Federal Register 40786, 18 July 2006

Ms. Johnson and Mr. Feldman:

BancorpSouth, through our office as its General Counsel, respectfully submits its comments on the above proposal to its primary regulators, the Federal Reserve and the FDIC.

BancorpSouth, Inc. is a financial holding company headquartered in Tupelo, Mississippi with approximately $11.8 billion in assets. BancorpSouth Bank, a wholly-owned subsidiary of BancorpSouth, Inc., operates approximately 270 commercial banking, insurance, trust and broker/dealer locations in Alabama, Arkansas, Florida, Louisiana, Mississippi, Tennessee and Texas.

These comments are based on "from the field" inquiries by the undersigned of BancorpSouth's personnel directly involved in the subject matter hereof or who may become directly involved, if the proposal is not adequately reigned in and streamlined. We offer some general comments followed by specifics tied to the portions of the proposal primarily related to credit and debit card issuers (of which BancorpSouth is both). Particular concerns exist concerning the "change of address" suggested procedures.

BancorpSouth is also a member of the American Bankers Association and the Financial Services Roundtable. BancorpSouth supports these trade group comment letters on this important topic, thanking these entities for their resources, expertise, and attention to detail. In addition to supporting those efforts, BancorpSouth does, however, ask to address some specific aspects of the proposal, reactionary admittedly from BancorpSouth personnel, but not believed to be unique. To the contrary, these comments appear supportive and representative of the more global industry response.

Overview

First and foremost, by recognizing that the proposed regulations are required by Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), such proposed regulations should only implement the FACT Act requirements and not delve beyond such, causing unnecessary burden, confusion, and duplicative efforts.

In this regard, we respectfully submit the proposal fails to fully take into account the synergies already gained by existing law and regulation, namely, the information security guidelines under the Gramm-Leach-Bliley Act (GLBA) and the Customer Identification Program requirements (CIP) under the Patriot Act. Indeed, a reading of the risk evaluation proposed procedure seems to mirror the concepts already in place under the Patriot Act's CIP requirements for financial institutions. Yet closely mirroring is not the same as tracking these requirements, causing confusion, i.e., "what's different?"; "what's new?"; "which one do you follow?" all of which appears to be unnecessary and duplicative.

In that the proposal is nearly identical to the factors already in place when BancorpSouth must open a new account, we respectfully submit that these factors being already in place are adequate safeguards. Extending the evaluation process to subsequent post-account opening events may not achieve the regulatory goal of reduced fraud, but instead, simply supply customer

inconvenience.

Address Related Issues

The sections of the proposal which discuss address discrepancies between what a financial institution has initially submitted in an initial credit bureau request and as to what may come back from a consumer reporting agency (and then in turn what the financial institution does to verify the discrepancies) are already covered by existing CIP procedures. Similarly, the items addressing "customer verification" on the front end are already included in existing financial institution CIP procedures. Simply put, the "red flag" items covered in 1-15 of Appendix J are already covered in one way or another in existing credit card application review processes.[1]

From a debit card perspective, address changes are only initiated after an account address is updated. Unless there is some way to do a mailer using an old address whenever a change is made to an account in a bank's main computer system, information technology personnel of BancorpSouth submit it would be most difficult to accomplish such using any current systems maintained by financial institutions. Indeed, BancorpSouth does have the technological ability to systematically produce letters to both a cardholder's current address and the requested new address. BancorpSouth submits, however, that the added expense of this process is not necessary due to the other processes already in place.

The proposed regulation states that banks are prohibited from issuing a card within 30 days of an address change unless they "access the validity" of the change of address request. Anticipating that this requirement would prohibit the bank from re-ordering a new card for a customer who has recently moved until some time after the "letter verification process" has been completed, creates a definite negative customer service impact for our customers.

As to "red flag" 16, the customer service staff, technology link, or other means to "tie in" an address change with a request for new or additional cards is problematic. Indeed, verification is made of the identity of persons requesting a change of address as is verification of persons seeking new or additional cards. These two transactions are simply not linked sufficiently to tie one request to the other. It should therefore be sufficient if reasonable procedures are in place to test the legitimacy of the specific request, be it address change or additional card request, when each such separate request is initially made.

---

[1]Most of the other items detailed in Appendix J also have processes and procedures "in place" to detect unusual occurrences, allowing the institution time to take appropriate action. Having the unnecessary burden to use the proposed regulations as a "check list" to see if you simply met regulatory requirements, all of which duplicate current procedures in place, tends to water-down the "in place" procedures, not equating to customer account safety.

As to address change "red flag" 17, it fails to take into account our most mobile society. Candidly and admittedly to be reactionary to the Fair Credit Reporting Act, we respectfully submit financial institutions already "over-report" address inconsistencies. Thus, rather than adding another "red flag" to the mix (see for example, flag 2), the FRCA needs to suffice or better said, revisit in regulatory form, as a clear, bright-line test, the effectiveness of such existing reporting. There is a reason that financial institution documents have almost always contractually had the right in favor of the bank to use the "last known address" for a customer. Undeliverable mail is too common an occurrence to be useful as an independent red flag standing alone. Simply put, it is all too common for customers to forget to notify us of a change of address, either directly or through postal service means.

Rest assured that BancorpSouth, like most card issuers, are "all about" fraud detection and prevention. While proprietary to a large extent, also rest assured that BancorpSouth and other financial institutions have in place several systems and processes to assist in fraud prevention that already help detect unusual activity on an account. We therefore respectfully submit that the "two letter verification process" is unneeded.

"Inactive" Accounts

The proposal would require customer notification when a transaction is made on an account which has been inactive for two years. We respectfully submit that this does not equate to an indication of potential identity theft. Indeed, many a customer uses their cards frequently, but others use credit cards for cash advances only, for travel only, to make emergency purchases, or to make large, non-routine purchases. Setting the "inactive" "flag" for such circumstances begs these questions: What will the financial institution do with those accounts? Decline them until verification is obtained from the customer (with again, negative impact to our customer)? And if one sends out some type of verification "after the fact," what assurance would this provide to the financial institution or the customer? Simply put, existing fraud prevention measures have adequate transaction monitoring systems in place that are designed to detect unusual activity. These measures allow card issuers to take appropriate action, all the while providing minimal negative customer impact. Adding these additional requirements will not only be burdensome, but non-customer friendly.[2]

---

[2]Indeed, being "all about" fraud prevention as detailed above amplifies that the credit card and debit card business takes this subject most seriously. (It stands to bear the brunt of the economic risk of fraud.) Having done so adequately under existing law and procedures, such requirements, if they appropriately mirror CIP programs, should fall on just credit card and debit card issuers. To the extent the proposal endeavors to address closed-end credit transactions, which we respectfully submit is unclear, the Agencies should definitively determine that closed-end credit arrangements are excluded from the "address red flags."

Unintended Civil Liability Consequences

True identity theft protection "begins at home." Education is the key as wrongdoers continue to utilize technology and other means to scam customers, all the while rarely finding true customer innocence from contributory negligence leading to the fraud. Yet these proposed rules place an unnecessary burden of "customer policemen" on the bank, not only potentially excusing customer behavior, but adding to the potential of civil liability of a financial institution, an unintended consequence, when otherwise the law may protect the bank.

Requiring the bank to do certain things, or document why it did not do a certain thing, may become the civil standards for "failure to do so" therefore be liable in court, to attorney generals, etc., not for identity theft prevention, but purely from failure to follow or adopt the various proposed provisions. Documenting merely to justify to an examiner why a financial institution has not adopted a particular "red flag" should be risk avoidance of the bank, not as a shield or sword for the customer. Thus at a minimum, the regulations should protect (not extend, imply or provide a plaintiff's expert with fodder for some policy or procedure equaling commercial unreasonableness) when financial institutions have instead, made good faith efforts to implement programs to comply with these provisions.[3]

Regrettably, existing legal protections for banks and their potential safety and soundness are ever being eroded by "customer police" type measures which tend to negate longstanding deposit law. The concepts under the Uniform Commercial Code, with decades of seasoning, for example, "failure to examine statements," "negligence contributing to a forgery," and the like get watered down or used offensively against the financial institution as customers will use these regulations to support claims that it is banks who are responsible, not themselves.

And regardless of the "program," does the bank find itself liable because it failed to adequately train staff as purportedly required by Section (D)(3). What possible relevance could there be for this non-statutory addition via regulation to require some form of specialized training just to have it be plaintiff's lawyer fodder that may be otherwise untenable under existing law. Funds protection measures already in place govern the matter (simply put, if it is unauthorized by the customer, generally, the customer has no responsibility). But what is one to do with conflicting signals from the regulations, namely, "relax your ID and verification requirements for CRA purposes, reach out to the community . . . ; make funds available under Reg CC, even if a

[3]Otherwise, this does not bode well for a financial institution now required to articulate a justification for its processes, as these proposals (just like the CIP rules), do not provide, but should provide a safe harbor. Even the Bank Secrecy Act's no private right of action becomes "iffy" under these proposals.

check has not made its way through the system. Yet here, the red flag program creates risk.

With the bank compelled to provide access to funds even though there is no way to know whether the item is legitimate or not, what now changes, if there is a return after a Reg CC authorized withdrawal? It should be the customer found to be in the best position to evaluate their own situation and assess the risk, not solely the bank, who by law, cannot prevent "sleep at the switch" customers from withdrawing funds. Yet with these proposals, customers will assert pattern and practice/habit and custom/commercial unreasonableness to say, "you bank, should have known" . . . and you failed to do something. Or, regardless of the 31 flags and their effect or preventive, if the institution just did not have adequate training, or being "written up" for failure to comply, risk exists, all the while the bank may have actually had nothing to do with the identity theft itself. It is not just creation of liability which causes concern here; it is customer avoidance of their own liability for returned items, unauthorized charges and the like based upon an unsubstantiated ascertain (but one which will "get legs") if banks are required to be the detectors of inappropriate account activity.

Director Involvement

It is important for the Board of Directors of BancorpSouth to set policy, including addressing risk management, but as particular to the latter, to quote from our risk management committee director chairman, "our job is to see that risk is being managed; not manage the risk ourselves." We believe this concept is supported by good corporate governance principals. Yet suddenly, the category of identity theft, not supported by the Act, is elevated to board-level policy involvement and approval. We submit that we should be able to designate the appropriate officials to oversee the identity theft risk as with other compliance and risk-related programs. Alternatively, any such board of director involvement needs to track and be consistent with the approach that was taken with the GLBA security standards.

BancorpSouth has quarterly Board of Directors meetings. Thus, be it from mere timing, or level of involvement and reporting, the fraudsters will be ahead of that game, necessitating management take quick action (albeit potentially outside any "board-approved" program). We therefore believe that board approval of such a program hinders the goals sought by the proposal when timing may be critical to address a particular fraud. Our directors are devoted but do not have specific fraud expertise nor should they be shouldered with such an obligation, when qualified staff are the appropriate ones to be identified to address same (with obvious material reports to the Board if and as necessary).

Regulatory Burden

While BancorpSouth personnel are unable to specifically respond to the asserted regulatory burden number of hours suggested by the proposal, immediate and strong reactions of "no way;" "unrealistic," were sounded. So much so that quite candidly, surveying BancorpSouth personnel to even respond by this comment comes close to meeting the hourly regulatory burden threshold pitched in the proposal. Suffice it to say that BancorpSouth is most fearful of a time consuming and expensive burden forthcoming if these proposals are not significantly reduced.

Conclusion

When one of BancorpSouth's career security and audit officers reviewed the subject proposals, she quickly stated, "This isn't about identity theft . . . this is garden variety, old timey fraud." Indeed, she was correct. Yet rather than any signification of ignoring any type of fraud, rest assured it is taken most seriously at BancorpSouth as it is at all financial institutions, but by blurring the lines between true identity theft versus all aspects of potential fraud, the educational goals of identity theft by regulators, the FBI, other law enforcement, and financial institutions themselves become clouded with mixed signals, and less than effective.

With that in mind, recognizing that one could easily construe the flags tied to specific notices *from* customers being beyond identity theft, these indeed are the ones welcomed: bright-line tests wherein the customers themselves, acting on their own devices of likely being involved in the transaction, meeting their own burdens of self-policing, did what they are supposed to do, notify their financial institution who then in turn should indeed then act. Such action, however, should be customer focused, systems related, and not "close the account or else" type reactions.

The financial institution has and should have an obligation to be proactive in this regard (for its own financial risk itself and reputational risk). It should not carry the extra burden of new checklists, new forms, new procedures, new reports. To the contrary, support banks in what they already endeavor to do in the category of fraud prevention and detection. Do not add extra burden to this already existing challenge.

Respectfully submitted,

PAT CALDWELL,
General Counsel

JPC/btw