Comerica Tower at Detroit Center
Corporate Legal Department
500 Woodward Avenue, MC 3391
Detroit, Michigan 48226
(313) 222-7464
(313) 222-9480 Facsimile

Julius L. Loeser
Chief Regulatory and
Compliance Counsel

By E-mail to regs.comments@federalreserve.gov September 18, 2006

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551

Re: Red Flags Rule (Docket No. R-1255)

Dear Ms. Johnson:

Comerica Bank, Detroit, Michigan, is writing to comment on the federal agencies' joint notice of proposed rulemaking concerning identity theft "red flags" and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). Comerica Bank is both a state member bank and a user of consumer reports and, thus, would incur substantial new duties if the proposed rule were to be adopted and, thus is directly affected by the proposal. Comerica Bank is a full service bank with total assets of $57.6 billion as of June 30; it provides banking services through branch offices in Michigan, California, Texas, Florida, and Arizona.

RISK-BASED AND FLEXIBLE

Comerica Bank, of course, strongly supports the national policy against identify theft evidenced by various provisions of FACTA. Identity theft is a serious problem, and Comerica Bank has actively worked to prevent identity theft. It was one of the original supporters of the banking industry's Identity Theft Assistance Center.

We also applaud the agencies' proposed adoption of an approach that is both flexible and risk-based. Obviously, different financial institutions conduct business in different ways and emphasize different services, service different customer bases, and flexibility enables a financial institution to tailor an identity theft program to its particular unique situation. Further, as the agencies recognize, fraud changes as man's ingenuity continually seems to counter new anti-fraud measures that are instituted from time to time.

ROLE OF BOARD OF DIRECTORS

Every important regulatory proposal usually includes a requirement that the board of directors or a committee thereof approve and at least annually review a program, be it information security, anti-money laundering, real estate lending, financial institution exposure, etc. Board and board committee agendas are already quite full with very important matters. As important as every new regulatory initiative

is, does each require board of director involvement? Might the agencies consider repealing older board approval and review requirements as new ones are added?

DEFINITION OF "ACCOUNT"

We appreciate that the definition of "account" that is proposed contemplates a continuing relationship; that is quite helpful. The proposed regulation gives examples of "accounts", such as credit card and deposit relationships. It would be helpful if the proposed regulation also gave examples of what is not an "account", e.g. sale of a cashiers check, a foreign exchange transaction, the issuance of a letter of credit, use of a bank's ATM.

DEFINITION OF "CUSTOMER"

The proposed definition of the term "customer" includes not only individuals, but also partnerships, corporations, and even governments. Implementation of the proposed regulation, if it only applied to individuals may be expected to be a major undertaking at most financial institutions. It will complicate implementation of the proposal enormously if financial institutions are to apply the program to customers who are not individuals as theoretically desirable as that might be. We are not aware of identity theft being a significant problem for persons other than individuals, and, if we have an accurate perception of the problem, that means that the additional burden that would be required to cover accounts of partnerships, corporations, and governments would be unnecessary at this time.

Of course, many of the "red flags" are based on information in consumer reports, and such reports will not be available for partnerships, corporations or governments.

As discussed below, the term "identity theft" would be defined broad enough to encompass garden variety fraud. If that definition is adopted, and customers are to include businesses, financial institutions will be responsible for preventing fraud on businesses. One example of such fraud that financial institutions would have to prevent that involves businesses and is not identity theft in the conventional sense, but is encompassed in the definition of "identity theft", is bookkeeper embezzlement where, in the small business context, a trusted bookkeeper controls the check stock and also reviews the monthly statements, and, thus, does not report forged checks he or she has stolen from the business. Under the Uniform Commercial Code, today, the depository bank has a defense because the business customer does not bring the fraud to the bank's attention within so many days after receipt of the monthly statement. The proposed regulation, if adopted as proposed, would give such business customers a claim that the bank had a duty to prevent the "identity theft" of the business and failed to do so. Irrespective of whether FACTA confers a private right of action, state unfair and deceptive practices statutes may well be interpreted to impose a legally enforceable duty on banks and liability to customers based on the proposed regulations. Counsel to defrauded business depositors will assert breach of such duty in actions intended to transfer the economic loss from the businesses to their banks.

DEFINITION OF "IDENTITY THEFT"

The proposed definition of the term "identity theft" would utilize the definition of the term in a rule adopted by the Federal Trade Commission ("FTC") in 2004. At the time of the adoption of that rule, we believe there was considerable criticism that the definition was too broad and included "garden variety" fraud unrelated to what is conventionally considered identity theft. Utilizing the FTC's definition of the term, while having, on its face, a certain logic, means that flaws in that definition would be compounded. One effect of the proposed regulation, as discussed below, may well be to make the nation's financial institutions responsible for the prevention of identity theft in the United States, which is no mean undertaking. To make that industry responsible for more, i.e. the prevention of fraud in the United States

would impose a task that hundreds of years of law enforcement resources has failed to achieve.

The proposed "red flags" include several examples of indices of fraud that have nothing to do with identity theft as the term is commonly understood. For example, "red flag" number 4 (documents presented for identification appear to have been altered) is, and long has been, an indicator of fraud, not identity theft, i.e. the presenter of the documents usually is attempting to pass himself or herself off as someone who may not exist, not trying to take the identity of someone else. Similarly, "red flag" number 7 (information on the identification is not consistent with information that is on file) is an indicator of fraud or forgery, not identity theft. Also, "red flag" number 10 (personal information is associated with fraudulent activity) has nothing to do with identity theft and everything to do with fraud. The same thing obviously can be said for "red flag" number 11 (personal information provided is of a type commonly associated with fraudulent activity).

Embezzlement is not identity theft, nor is forgery, nor theft of checks or credit cards. These have all long been crimes. We would respectfully suggest that a better definition of the term "identity theft" than the FTC's definition would be "the opening of an account by the use of another person's identifiers without that person's authorization". There is no question that identity theft is fraud, but it is a subset of fraud. Financial institutions work hard to protect their customers from fraud of all types. However, if financial institutions are to have a legal duty to prevent it, that duty should be limited to identity theft, not extend to embezzlement, forgery, check theft, credit card theft, and most types of fraud.

DEFINITION OF "RED FLAGS"

The statute provides that "red flags' are only to be activities that indicate the possible existence of identity theft. Our experience is that certain of the activities listed as "red flags" have not really been indices of identity theft and that is after extensive investigation in each case. For example, "red flag" number 1 (fraud alert included in a consumer report) may not evidence real identity theft. If the agencies have sufficient data, they might be able to specify what types of activity giving rise to fraud alerts is more likely to evidence identity theft than others and could refine "red flag" number 1.

Other "red flags" appear to be too broad. "Red flags" numbers 2 (notice of address discrepancy is provided by a consumer reporting agency), 6 (information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification), 7 (other information on the identification is not consistent with information that is on file), 8 (personal information provided is inconsistent when compared against external information sources), and 9 (personal information is internally inconsistent) would be triggered by a mere inadvertent typographical error and, in each such case, would require an investigation. Might it be possible to exempt obvious typographical errors?

Another "red flag" that we believe is a poor indicator of identity theft is number 13 (the person opening the account fails to provide all required information on an application). Thus, a failure to include a zip code would raise a "red flag" triggering an identity theft investigation. Would it be possible for the agencies to be more specific and limit the types of information, absence of which would raise an identity theft "red flag".

Yet other "red flags" that have been proposed, but which we do not believe are indicators of identity theft, are "red flags" numbers 18(b) (customer fails to make the first payment or makes an initial payment but no subsequent payments) and 19 (a) (nonpayment when there is no history of late or missed payments). Obviously, payment defaults unfortunately are part of the lending business, and any history of late or missed payment begins with a nonpayment. Rarely is it evidence of fraud, much less evidence of identity theft.

Similarly, "red flag" number 20 (an account that has been inactive for a reasonably lengthy period of time is used) is a poor indicator of identity theft if the account is a revolving equity account as that is the typical pattern of usage for such accounts.

The problem with "red flags" that are not likely indicators of identity theft is that the proposed regulation requires an investigation each time a "red flag" is raised. If a "red flag" is not a good indicator of identity theft, all financial institutions will be required to conduct costly unnecessary investigations that benefit no one.

IDENTITY THEFT "PREVENTION"

Section 114 of FACTA authorizes the agencies to prescribe regulations requiring financial institutions to establish reasonable policies and procedures for implementing the guidelines to "identify" possible risks. Nowhere does it use the verb "prevent". The proposed regulations appear to go beyond the statute to impose obligations on institutions not only to identify, but also to prevent, identity theft. While one might debate whether, logically, identification has any purpose other than to assist in prevention, a duty to identify to assist prevention is much less of a duty than a duty actually to prevent identity theft. The financial services industry should not become the nation's guarantor and insurer against identity theft. However, if the proposed regulation is adopted as proposed, it will be, as courts throughout the country will translate a failure to comply with the regulation's duty to prevent identity theft as an unfair or deceptive practice under state unfair and deceptive practices statutes. That was not Congress' intent in Section 114 as evidenced by the language of the statute. The regulation should require Identity Theft Identification Programs, not Identity Theft Prevention Programs.

THE "RED FLAGS"

Identification of many of the proposed "red flags" will require costly system changes if identification is possible at all. For example, "red flag" number 7 (other information on the identification is not consistent with information that is on file, such as a signature card) implies that banks will be expected to check signatures, a practice in which most banks rarely engage. "Red flag" numbers 10 (a) and (b) (address or phone number on an application is the same as an address provided on a fraudulent application) would require extensive systems changes as most banks currently do not compare past applications to current applications and may not even have other than manual means of doing so (to the extent they even maintain copies of past applications). "Red flag" number 11 (personal information provided is of a type commonly associated with fraudulent activity, e.g. fictitious address, invalid phone number) would require financial institutions to expand the identification verification they currently undertake as today they have no practical way to determine if an address is fictitious. Similarly, "red flag" number 12 (address, SSN, or home or cell phone number provided is the same as that submitted by other persons) would also require expansion of current identification verification efforts as financial institutions generally do not normally track customer cell phone numbers. Further, to the extent that members of our highly mobile society frequently move and change addresses and telephone numbers, tracking such information reliably would be a particularly difficult undertaking. "Red flag" number 18 (a) (majority of available credit is used for cash advances or merchandise easily convertible into cash (e.g. electronics equipment or jewelry)) is another example of activity that banks generally do not currently monitor as most banks do not track what purchases card holders actually make. "Red flag" 19 (b) (material increase in the use of available credit) is another "red flag" that most financial institutions currently do not monitor, but would have to start monitoring if the regulation became final. While some financial institutions have the sophisticated the sophisticated technology to detect changes in cellular telephone call patterns, many financial institutions generally have no way today of ascertaining the existence of "red flag" number 19 (e) (material change in telephone call patterns in connection with a cellular phone account). Is the bank to consider from whence a telephone call originates and consider it a "red flag" if a new number is used? We also believe that many

financial institutions do not currently have a mechanism to identify "red flag" number 26 (the name of an employee of the financial institution has been added as an authorized user on an account). Similarly, most financial institutions do not track for "red flag" number 30 (unusually frequent and large check orders in connection with a customer's account). Indeed, many financial institutions delegate check orders to outside vendors and thus currently do not have information as to the frequency or size of customer check orders. Of course, much of this will require expensive systems changes, such as the creation of software to compare each new customer's address, SSN, home phone number, and cell phone number to those of existing customers.

In addition, proper identification and response likely will cause significant management and organizational changes at many institutions. Currently, different proposed "red flags" might be identified by different business units, but identification of some individual "red flags" will require coordination and management of multiple business units; and the entire effort of identifying multiple red flags will certainly require centralized coordination and management not present in most financial institutions.

Some legal changes would facilitate the ability of financial institutions to identify "red flags". For example, a number of proposed "red flags" would be triggered by information in consumer reports. However, one's authority to order a consumer report today is highly limited by the Fair Credit Reporting Act ("FCRA") generally to extending credit, employment, or insurance. If the FCRA were amended to permit a financial institution to order a consumer report in order to identify or investigate possible identity theft, financial institutions would be better able to help prevent identity theft[1].

TIMING OF IMPLEMENTATION

We believe, as discussed above, that implementation of the proposed regulation will require substantial system, management, and organizational changes. Thus, we would respectfully urge that the transition period be as long as possible and that the implementation date be as late as possible. We estimate that we would need eighteen to twenty-four months after adoption of a final regulation to make the system, management, and organizational changes the final regulation would require if it were to be adopted with substantially the same tenor has this proposal.

Thank you very much for this opportunity to express our views on this important issue of public policy.

Best wishes,

Julius L. Loeser

[1] The FCRA also permits the ordering of a consumer report for a legitimate business purpose in connection with a transaction initiated by the consumer who is the subject of the report, and, thus, the FTC arguably could adopt a rule providing that "legitimate business purpose" includes investigating potential identity theft, but, if the transaction truly involved identity theft, the transaction would not have been initiated by the consumer who was the subject of the report. Thus, an amendment of FCRA would appear to be needed to accomplish this.