

October 14, 2003

Public Information Room  
Office of the Comptroller of the Currency  
250 E Street, SW  
Mail Stop 1-5  
Washington, D.C. 20219  
Attention: Docket No. 03-18

Ms. Jennifer J. Johnson  
Secretary  
Board of Governors of the  
Federal Reserve System  
20<sup>th</sup> Street and Constitution Ave., NW  
Washington, DC 20551  
Attention: Docket No. OP-1155

Robert E. Feldman  
Executive Secretary  
Attention: Comments/OES  
Federal Deposit Insurance  
Corporation  
550 17<sup>th</sup> Street, NW  
Washington, DC 20429

Regulation Comments  
Chief Counsel's Office  
Office of Thrift Supervision  
1700 G Street, NW  
Washington, DC 20552  
Attention: No.03-35

Re: Interagency Guidance on Response Programs for Unauthorized Access to  
Customer Information and Customer Notice

Dear Sirs and Madams:

The following comments are provided on behalf of Comerica Incorporated, a \$59 billion bank holding company located in various states including California, Florida, Michigan and Texas. Comerica appreciates the opportunity to comment on this important proposal.

Comerica believes that protecting customer information is of paramount concern. It is the foundation of trust that a customer has with its financial institution. With that trust and communication as the basis of the customer relationship we do not believe the industry needs additional regulation to communicate this trust to its customers.

The basis of the trust is how a customer is treated and communicated to by its financial institution. Specific remedies are not needed. The approach should be to measure the success of the existing "risk-based" process that all financial institutions take with their customers.

Regulators can and have the responsibility to measure this "risk-based" approach during their examinations. Present situations, which dictate a notice to the regulator outside of the examination, are presently handled through the Suspicious Activity Report (SAR) process. Regulators who desire further communication should modify the SAR guidelines to capture the additional information.

A customer's trust with a financial institution is built upon the framework of protecting sensitive customer information. The definition of Sensitive Customer Information needs to be reviewed. Having the specific rigid remedies outlined in the proposal may actually result in expectations of the customer being raised that can no longer be met under today's "risk-based" driven notification which is followed in the industry.

Finally, any effective guidance in this area must allow for state laws to be preempted. The sensitive customer information that is to be protected by this proposal is easily moved over state lines in seconds. It is time regulation recognizes the issue as a national/global issue rather than a state issue. Without preemption the ability to conduct nationwide activities in a consistent manner is in question.

#### Additional Regulation is Not Necessary

Section 501(b) of the GLBA provides standards for safeguarding customer information. In addition, if the proposal is an attempt to deal with identity theft and fraud issues in the marketplace, the industry has taken a proactive approach in this area. Comerica has created its own identity theft response program. Finally, the biggest issue in the fight against Identity Theft at this time is the lack of sufficient resources on a local basis to prosecute and jail those who conduct this activity. Identification of the issues is being done well through the industry's own risk-based processes. If the ability to prosecute those who conduct Identity Theft is not improved we would argue that the proposal will actually make the situation worse and not better.

#### The Existing "Risk-Based" Approach is working well

Regulators should acknowledge that the industry has faced these issues in the past and the issue is not new to the industry. The industry should continue to deal with these issues in the "risk-based" approach and avoid delineating so many specific or pre-determined requirements for notifying customers and regulatory agencies.

The measurement of the existing processes would be appropriate during the examination process. Perhaps after a longer period of time the examination teams could share the "best practices" that they see in their examinations. This would be more practical in today's world rather than rigid guidance. The industry has been proactive in creating comprehensive response programs and will continue to meet the needs of their customers on an ongoing basis.

#### Notice to Regulators

The proposal mandates that an institution should promptly notify its primary federal regulator when it becomes aware of an incident that could result in substantial harm or inconvenience to its customers. Access that could result in inconvenience is a very low threshold. Virtually every incident may require notification. Any incident could possibly result in substantial harm to our customer. We understand and agree that regulators need to be informed of significant incidents. However, notification should only occur when an incident poses a significant risk of substantial harm to a significant number of our customers.

#### Give More Flexibility in Determining A Course of Action

As previously stated, the present "risk-based" approach used by financial institutions provides the flexibility needed. The proposal requiring the customer's agreement to a course of action may actually impede the ability to deal with an issue in the most efficient manner. The proposal does not take into account that a financial institution may have followed a course of action for which customer consent is not typically required or requested. The proposal should not impose a new obligation in this area. A customer consent requirement may be a disincentive to innovation and attempts by institutions to try new mechanisms for securing accounts. The proposal does not anticipate the legal barriers that may arise when agreement on action is required. In addition, there are large operational impacts on financial institutions if they had to notify or communicate with all customers or groups of customers that might be impacted from a security breach and ask the customers if they agreed with a particular course of action.

#### Customer Notice

The present proposal does not take into account the real question, which is whether or not the notice given to customers would provide a meaningful opportunity to help prevent or reduce the harm to those customers and/or the institution. Ultimately, this is what financial institutions need to be allowed to consider when deciding whether or not to notify a customer.

#### Determining Which Customers to Notify

The proposal is very broad regarding the customers who are to be notified. We would ask that financial institutions be given the flexibility to use an alternative notice in the case where there is a large number of customers to notify. Alternatives would include e-mail, postings on the financial institution's web site and other news media outlets.

#### Customer Reaction

Strict notice to customers will cause anxiety on the part of customers. We may not be able to adequately respond to customers' inquiries about the likelihood of financial loss

resulting from an identity theft. As a result, customers may unnecessarily change passwords, cancel accounts or take other actions after receiving a notification. Alternatively, if notice is not tied to risk, customers may under-react to notices, become less responsive and fail to take the necessary action at the appropriate time. Again, the present process of using "risk-based" notification allows the appropriate balance.

Notice Should Only Apply to Sensitive Customer  
Information under the Control of a Financial Institution

Notice should only apply to sensitive customer information under the control of a financial institution. Where the institution has contracted with a third party to carry out some or all of its information technology functions, the institution continues to control the sensitive customer information and should provide any notification. However, where the financial institution provides sensitive customer information to federal, state or local government entities, and that entity suffers a security breach, the financial institution should not be required to notify customers of such an incident. The proposal should make it clear that once the information is sent to a government entity, for example, the information is no longer under the control of the financial institution. The focus should be on the "control" of information rather than the ownership of information because, in any given situation, ownership of sensitive customer information may be less clear than control of the information.

Definition of Sensitive Customer Information

The key element in this definition is whether or not particular information materially increases the likelihood that a particular consumer would become the victim of identity theft or fraud. For instance:

1. "Encrypted information" should not be considered sensitive information unless there was reason to believe the encryption had been or could be broken. Not including encrypted data in the definition of sensitive customer information, may motivate companies to continue efforts to encrypt sensitive data. Financial institutions should consider whether or not the data is encrypted when conducting their risk-based analysis of whether or not the customer will be harmed.
2. "Account numbers" should not always be considered sensitive information. For example, the account number for an installment loan is of no use to potential hackers. Often, account numbers without access codes are useless unless the account can be debited without any access code or device. This should be addressed in the proposed Guidance by only including that information which could lead to access to a customer's financial information.

Sirs & Madams  
October 14, 2003  
Page 5

3. "Publicly available information", defined as information that is lawfully made available to the general public from federal, state, or local government records should also be excluded from the definition of sensitive data.

State Laws Should Be Preempted

Without preemption interstate commerce will be impeded. For instance, the possibility exists for a customer to receive 51 different versions of notice (50 states and the new GLBA notice.) This is impractical and burdensome .

Conclusion

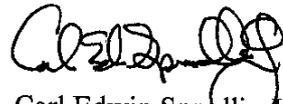
Comerica believes that another draft of the proposed Guidance needs to be drafted and circulated. It should be of true guidance with best practices cited but with the flexibility to allow financial institutions to use their existing "risk-based" process. The process needs enhancing but it is not broken. The proposal as written will not increase prosecutions for Identity Theft. As written, it will create less trust by our customers in a process, which is extremely complex.

Thank you again for the opportunity to comment on this important issue.

Sincerely,



Julius L. Loeser  
Senior Vice President  
Corporate Legal



Carl Edwin Spradlin Jr.  
First Vice President  
Corporate Public Affairs