Kenneth S. Spirer
First Vice President and
Assistant General Counsel

Office of General Counsel

222 Broadway
17th Floor
New York, New York 10038
212 670 0225
207 879 7112 Maine
FAX 212 670 4519
kenneth_spirer@ml.com

Merrill Lynch

37

August 25, 2000

Office of the Comptroller of the Currency
Communications Division
250 E Street, SW
3rd Floor
Washington, D.C. 20219
Attention: Docket No. 00-13

Jennifer J. Johnson, Secretary
Board of Governors of the Federal Reserve System
20th & C Streets, NW
Washington, D.C. 20551
Attention: Docket No. R-1073

Robert E. Feldman
Executive Secretary
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, D.C. 20429
Attention: Comments/OES

Manager Dissemination Branch
Information Management and Services Division
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552

Ladies and Gentlemen:

Merrill Lynch is pleased to respond to the request for comments on the recently issued proposal that would, if adopted, establish standards for safeguarding customer information. These proposed Guidelines have been issued to implement Sections 501 and 505(b) of the Gramm-Leach-Bliley Act. Under the provisions of Section 501 of the

Gramm-Leach Bliley Act, federal banking agencies are required to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to administrative, technical, and physical safeguards for customer records and information. Section 505(b) requires the agencies to implement these standards in the same manner to the extent practicable, as standards prescribed pursuant to Section 39(a) of the Federal Deposit Insurance Act.

Merrill Lynch agrees that financial institutions should establish standards for the safeguarding of customer records and information and, subject to our comments below, we support the general thrust of these proposals. The agencies have asked a number of questions in the release and we have set forth our views on certain of these questions.

Guidelines vs. Regulations

We recommend that these standards be published as guidelines rather than as regulations since doing so will allow financial institutions greater flexibility to tailor their policies and establish procedures to more appropriately reflect their size and business model.

Definitions

We suggest that the definition of "customer" be limited to individuals to remain consistent with the coverage of the Gramm-Leach-Bliley Act.

Corporate Information Security Officer

While we agree with the concept of a Corporate Information Security Officer for banking institutions, it may be premature to require that every banking institution establish such a position. Depending on the size and structure of the banking institution, it may not be necessary to appoint a Corporate Information Security Officer.

Board Reporting

The subject of protecting customer records and information is extremely important for a banking institution and should be brought to the attention of the financial institution's Board of Directors on a regular basis. The frequency of such reporting may depend, in part, on the size of the institution and the nature of its information security activities. In our view, reports on a semi-annual basis would be appropriate for most institutions. Further, we believe that an institution's Board should be authorized to delegate its authority to receive these reports to a committee of the Board that would, in turn, provide a summary of this activity to the full Board as appropriate.

Specific types of tests

Since the type of tests need to be tailored to an institution's specific risks, structure and lines of business, we do not believe that dictating the required types of tests is appropriate. We also would urge the agencies to allow institutions the flexibility of using any resources, whether internal or external, to conduct the necessary tests. If internal resources are utilized, it would be appropriate, however, to have these tests performed by individuals in an organization who have no reporting or functional responsibilities for the activities being tested.

Outsourcing arrangements

We agree generally with the statement that an institution should exercise appropriate due diligence, in managing and monitoring its outsourcing arrangements, in order to confirm that its service providers are implementing an effective information security program to protect customer information. When the service provider for a depository institution also maintains the direct client relationship, such as a deposit broker that places brokered deposits for its clients and maintains or processes depositor information, the service provider should only be required to meet the standard of

customer protection imposed by its own functional regulator. A depository institution using a service provider to maintain or process customer information, or otherwise granting such service provider access to customer information, should be deemed to have exercised appropriate due diligence in managing and monitoring this outsourcing arrangement if the service provider is subject to regulatory standards established by its own functional regulator, and the service provider complies with the customer information protection rules or requirements of that functional regulator. While we agree that institutions should carefully monitor their service providers, the Guidelines should not specify contractual provisions requiring service provider performance standards since each institution, and its arrangement with a service provider, may be different.

We hope that these comments have been helpful. If you have any further questions please do not hesitate to contact the undersigned at 212-670-0225.

Very truly yours,

Kenneth S. Spirer