CLIENT MEMORANDUM

PRIVACY SAFEGUARD REQUIREMENTS OF THE SEC, NCUA, OCC, TREASURY, FEDERAL RESERVE SYSTEM, FDIC, OTS, AND FTC

The Gramm-Leach-Bliley Act ("GLB" or "Act"), passed in 1999, requires that certain federal regulatory agencies issue standards governing the administrative, technical, and physical safeguarding of customer records and information by financial institutions. On January 30, 2001, the National Credit Union Administration ("NCUA") issued its final guidelines on privacy safeguard protections, and on February 1, 2001, the Office of the Comptroller of the Currency ("OCC"), the Secretary of the Treasury ("Treasury"), the Board of Governors of the Federal Reserve System ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS") jointly adopted final guidelines on safeguarding customer information. The guidelines adopted by all of these agencies are identical (collectively, the "Interagency Guidelines"). Section I of this memo summarizes the Interagency Guidelines. The Securities and Exchange Commission ("SEC") submitted its final rules on safeguarding customer information on June 22, 2000. Section II of this memo summarizes the SEC's rules. The Federal Trade Commission ("FTC") recently proposed its safeguard rules and is accepting comments until October 9, 2001. Section III of this memo describes the FTC's Notice.

Because the privacy rules or proposed rules are far-reaching in scope and require significant changes to covered institutions' information practices, organizations should determine whether they are subject to the rules or proposed rules and, if so, take immediate steps to ensure compliance in order to avoid potentially significant liability.

I. SAFEGUARDING RULES OF THE NCUA, OCC, TREASURY, BOARD, FDIC, AND OTS.

A. Purpose and Scope of the Safeguard Rules and the Jurisdiction of the Agencies.

The Interagency Guidelines implement Sections 501 and 505(b)(2) of the GLB. They set forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Interagency Guidelines apply to member information maintained by or on behalf of the following institutions per agency jurisdiction:

NCUA: The Interagency Guidelines apply to all natural person credit unions, as well as all corporate credit unions that have a natural person member. However, the

Interagency Guidelines do not apply to any corporate credit union that does not afford membership to a natural person.

OCC: The Interagency Guidelines apply to national banks, as well as federal branches and federal agencies of foreign banks, and the subsidiaries of any national bank, federal branch, or federal agency of a foreign bank (with the exception of brokers, dealers, persons providing insurance, investment companies, and investment advisers).

The Board: The Interagency Guidelines apply to state member banks and their nonbank subsidiaries and bank holding companies (with the exception of brokers, dealers, persons providing insurance, investment companies, and investment advisors). In addition, the Interagency Guidelines apply to edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of a foreign bank.

FDIC: The Interagency Guidelines apply to entities over which the FDIC has authority, including banks insured by the FDIC (other than members of the Federal Reserve System), insured state branches of foreign banks, and any subsidiaries of such entities (with the exception of brokers, dealers, persons providing insurance, investment companies, and investment advisers).

OTS: The Interagency Guidelines apply to savings associations the deposits of which are FDIC-insured, and any subsidiaries of such savings associations (with the exception of brokers, dealers, persons providing insurance, investment companies, and investment advisers).

B. Preservation of Existing Authority.

The Interagency Guidelines make clear that nothing in the final rules limits in any way the authority of any individual agency to address unsafe or unsound practices, violations of law, unsafe or unsound conditions, or other practices.

C. Definitions of Key Terms.

The Interagency Guidelines adopt definitions of key terms that relate to the privacy protection policies. All other terms are defined in accordance with applicable agency rules and statutes.

1. Board of Directors: The body controlling an entity's operations. In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency of a foreign bank.

2. Customer: A consumer who has established a continuing relationship with an institution under which the institution provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes. "Customer" does not include a business, nor does it include a consumer who has not

established an ongoing relationship with a financial institution (e.g., an individual who merely uses an institution's ATM or applies for a loan).

3. Customer Information: Any record, data, or file containing nonpublic personal information about a Customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the entity.

4. Customer Information Systems: Any methods used to access, collect, store, use, transmit, protect, or dispose of Customer Information.

5. Service Provider: Any person or entity that maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to the entity.

6. Subsidiary: Any company controlled by an entity, except a broker, dealer, person providing insurance, investment company, investment advisor, insured depository institution, or subsidiary of an insured depository institution.

D. Standards for Safeguarding Customer Information.

1. Information Security Program. Each entity must implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the entity and its subsidiaries and the nature and scope of its activities. Although all parts of the entity are not required to implement a uniform set of policies, all elements of the information security program must be coordinated. An entity also must ensure that each of its Subsidiaries is subject to a comprehensive information security program. The entity may fulfill this requirement either by including a Subsidiary within the scope of the entity's comprehensive information security program, or by requiring the Subsidiary to implement a separate comprehensive information security program in accordance with the guideline standards.

2. Objectives of the Information Security Program. The information security program must be designed to ensure the security and confidentiality of Customer Information, and protect against any anticipated threats or hazards to the security or integrity of such information. Additionally, the program must protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any Customer.

E. Development and Implementation of an Information Security Program.

1. Approval by the Board of Directors. The Board of Directors or an appropriate committee of the Board of Directors must approve the entity's written information security program and oversee the development, implementation, and maintenance of the

program. The Board of Directors must assign specific responsibility for the program's implementation and for the review of reports from management.

2. Assess Risk. Each entity must identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of Customer Information or Customer Information Systems. Further, an entity must assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of Customer Information. An entity also must assess the sufficiency of policies, procedures, Customer Information Systems, and other arrangements in place to control the identifiable risks.

3. Manage and Control Risk. Each entity must design its information security program to control the identified risks, commensurate with the sensitivity of the information and the complexity of the entity's activities. Consideration must be given to the following security measures, and an entity must adopt those which are deemed appropriate:

a. System Access Controls. Measures designed to limit access to Customer Information Systems. Such measures shall include controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing Customer Information to unauthorized individuals who may seek to obtain this information through fraudulent means.

b. Access Restrictions at Physical Locations. Measures protecting access to sites containing Customer Information. Examples include limiting access to buildings, computer facilities, and records storage facilities only to authorized individuals.

c. Encryption. Measures to encrypt electronic Customer Information, including information in transit or in storage on networks or systems to which unauthorized individuals may have access.

d. Modification Protections. Measures designed to ensure that Customer Information System modifications are consistent with the entity's information security program.

e. Personnel Security. Measures implementing dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to Customer Information.

f. Monitoring Systems and Procedures. Measures that will detect actual and attempted attacks on or intrusions into Customer Information Systems.

g. Response Programs. Measures that specify actions to be taken when the entity suspects or detects that unauthorized individuals have gained access to Customer

Information Systems, including appropriate reports to regulatory and law enforcement agencies.

h. Damage Protection. Measures that will protect against destruction, loss, or damage of Customer Information due to potential fire and water damage or technological failures.

Additionally, each entity must train staff to implement the entity's information security program. An entity must regularly test the key controls, systems, and procedures of the program. Tests should be conducted in accordance with the risk assessed and should be reviewed by third parties or staff independent of those who develop or maintain the security programs.

4. Oversee Service Provider Arrangements. Each entity must exercise appropriate due diligence in selecting its Service Providers and require its Service Providers by contract to implement appropriate measures designed to meet the objectives of the Interagency Guidelines. Additionally, when deemed appropriate in consideration of risk, an entity must monitor its Service Providers to confirm that they have satisfied their privacy protection obligations. This monitoring should include reviews of audits, summaries of test results, or other equivalent evaluations of Service Providers.

5. Adjust the Program. Each entity must monitor, evaluate, and adjust, as appropriate, its information security program in light of any relevant changes in technology, the sensitivity of its Customer Information, internal or external threats to Customer Information, and the entity's own changing business arrangements. Any mergers, acquisitions, alliances, joint ventures, outsourcing arrangements, and changes to Customer Information Systems will warrant a reevaluation of the information security program.

6. Report to the Board of Directors: An entity must report to its Board of Directors or an appropriate committee of the Board of Directors at least annually. This report must describe the overall status of the information security program and the entity's compliance with the Interagency Guidelines. The reports should discuss material matters related to its program, addressing issues such as: risk assessment, risk management and control decisions, Service Provider arrangements, test results, security breaches or violations and management's responses, and recommendations for changes in the information security program.

F. Implementation of the Standards.

1. Effective Date. Each entity was required to implement an information security program pursuant to the Interagency Guidelines by July 1, 2001.

2. Grandfathering for Service Providers. There is a two-year grandfathering provision for agreements with Service Providers. Until July 1, 2003, a contract that an entity entered into with a Service Provider, on or before March 5, 2001, to perform services or to function on its behalf, satisfies the provisions of the Interagency Guidelines, even if the contract does not include a requirement that the Service Provider maintain the security and confidentiality of Customer Information.

G. Remedies for Ensuring Compliance with the Interagency Guidelines.

While specific remedies for noncompliance were not implemented, each regulatory agency, through its general enforcement authority, may determine that a covered entity has failed to satisfy the safety and soundness standards contained in the Interagency Guidelines. Such a finding must be based on evidence derived from an examination or inspection, or on any other information that becomes available to the agency through its own auditing procedures or due to individual complaints.

II. SAFEGUARDING RULES OF THE SEC.

A. Jurisdiction of the SEC.

The SEC's rules govern brokers, dealers, investment companies, and investment advisers that are registered with the SEC. Insurance providers are covered only if they offer an insurance product that is also a security. Additionally, all foreign (nonresident) brokers, dealers, investment companies, and investment advisers that are registered with the SEC are covered by the SEC's privacy rules. The rules do not apply to foreign (nonresident) brokers, dealers, investment companies, and investment advisers that are not registered with the SEC.

B. Standards for Safeguarding Customer Information.[1]

1. Application of the Rules. The rules adopted by the SEC apply only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes. The SEC rules do not apply to information about companies, or about individuals who obtain financial products or services primarily for business, commercial, or agricultural purposes.

2. Safeguard Rules. Every broker, dealer, investment company, and investment adviser registered with the SEC must adopt policies and procedures that address

---

[1] The SEC defines the term "Customer" in the same manner as the Interagency Guidelines. In contrast, the SEC does not define the term "customer records and information," as discussed in this section; however, the purpose of the Act and the SEC's rules is to protect the nonpublic personal information of Customers.

administrative, technical, and physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to (a) ensure the security and confidentiality of customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any Customer.

3. Effective Date. Each covered entity was required to implement an information security program by July 1, 2001.

4. Remedies. The SEC did not implement specific remedies for noncompliance; however, through its general enforcement authority, it may determine that a covered entity has failed to satisfy the safeguard requirements. Moreover, information concerning noncompliance may be filed with the SEC by individuals.

III. FTC'S PROPOSED SAFEGUARD RULES.[2]

A. Jurisdiction of the FTC.

The FTC's jurisdiction extends to those financial institutions that are not otherwise regulated by one of the other agencies discussed above. Those financial institutions covered by the FTC's rules include, but are not limited to: nondepository lenders, consumer reporting agencies, data processors, courier services, retailers that extend credit by issuing credit cards to consumers, personal property or real estate appraisers, check-cashing businesses, and mortgage brokers.

B. Standards for Safeguarding Customer Information.

The FTC's rules are still in the proposal stage. **Interested parties may file comments with the FTC by October 9, 2001.** The FTC's proposed rules would require covered financial institutions to develop a comprehensive written information security program to ensure that they safeguard their Customers' nonpublic personal information. The FTC envisions a "highly flexible" standard, under which each institution would be allowed to tailor its program to its size and complexity, the nature and scope of the activities in which it engages, and the sensitivity of any Customer Information it collects and maintains. The FTC will not require the program to be set forth in a single document, as long as all parts of the program are coordinated and can be identified and accessed easily.

---

[2] The FTC's definition of "Customer" and its proposed definition of "Customer Information" are identical to the Interagency Guidelines' definitions. In addition, the FTC's proposed definition of "Service Provider" is very similar to the Interagency Guidelines definition of "Service Provider," except the FTC definition, if adopted, would extend to Service Providers "receiving" Customer Information.

C. Implementation of an Information Security Program.

1. Designate Employee Coordinators. To ensure accountability for compliance with the rules, financial institutions would have to designate an employee or employees to coordinate their information security program.

2. Assess Risk. Financial institutions would need to identify reasonably foreseeable internal and external risks to the security and integrity of Customer Information that could result in the unauthorized disclosure, misuse, or other compromise of such Customer Information. At a minimum, these institutions would have to undertake risk assessments of their (a) employee training and management; (b) information systems, including information processing, storage, transmission, and disposal; and (c) prevention and response measures for attacks, intrusions, or other system failures. In addition, institutions would have to assess the sufficiency of any safeguards in place to control identified risks.

3. Design Risk Control. After identifying risks, financial institutions would have to design and implement information safeguards and procedures to control the risks and regularly test or otherwise monitor the effectiveness of such safeguards and procedures.

4. Oversee Service Providers. Financial institutions also would be required to ensure that the Service Providers they select and retain are capable of maintaining safeguards and that their Service Providers, through contract, implement and maintain such safeguards.

5. Evaluate and Adjust Program. Periodically, financial institutions would have to evaluate and adjust their security programs in light of changes in technology; their own operations or business arrangements, such as mergers and acquisitions, alliances and joint ventures outsourcing arrangements, or changes in the services provided; new or emerging internal or external threats to information security; or other circumstances that give them reason to know that their information security programs are vulnerable to attack or compromise.

D. Effective Date of the Rules.

The FTC proposes to require each financial institution subject to the FTC's jurisdiction to implement an information security program not later than one year from the date on which final rules are issued. However, it asks the public to comment on whether one year is an appropriate amount of time for covered entities to come into compliance. In addition, the FTC asks whether the rules should contain a transition period to allow the continuation of existing contracts with Service Providers, even if those contracts would not satisfy the rules' requirements.

Remedies. The FTC may employ its auditing or complaint process to enforce its rules. While the FTC has not proposed specific remedies for noncompliance, it may use its general enforcement authority to ensure compliance with the rules it implements.

IV. CONCLUSION.

The existing GLB rules and proposed FTC rules described above cover a broad array of financial institutions and impose complex regulations regarding the safeguarding of customer records and information. Organizations should carefully assess whether they are covered by the rules or proposed rules and, if so, bring their internal information systems into compliance in order to avoid potentially significant liabilities. Organizations subject to the FTC's jurisdiction may also want to file comments on the FTC's proposed rules by October 9, 2001.

If you have any questions concerning the Gramm-Leach Bliley Act or need any further information, please contact Frank Buono (202) 429-4749, Angie Kronenberg (202) 429-4726, Jeneba Ghatt (202) 429-4727, or Patrick Sullivan (202) 429-4706.

Willkie Farr & Gallagher is headquartered at 787 Seventh Avenue, New York, New York 10019. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111.

September 24, 2001