By Hand and by E-Mail

October 9, 2001

Secretary
Federal Trade Commission
Room 159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule, 16 CFR Part 314 - Comments

Dear Sir:

This comment letter is jointly submitted by the Education Finance Council and the National Council of Higher Education Loan Programs, Inc. These organizations represent most of the financial participants in the Federal Family Education Loan Program (the "FFELP"), the largest federally sponsored education loan program. Many members of these organizations also participate in supplemental, fully private, education loan programs.

We have reviewed with interest your proposed rule published in the Federal Register on August 7. In your notice of proposed rulemaking, you identified a number of specific issues for comment. In response, we have two comments that we would like to highlight upfront, and additional comments on some of your requests that deal with issues not covered in our two general comments.

First, we want to express our appreciation for the fact that, for the most part, the proposed rule sets forth requirements that are flexible enough to fit the circumstances of our members, who are of many organizational types (for-profit, nonprofit, state entities) and sizes. Though we have comments on some of the more specific aspects of the proposals, we want to commend the Commission for its overall approach. We should say as a general matter, however, that we likely would object to amendments to the proposed rules that would make them more prescriptive.

Second, we are concerned about potential duplicative requirements being imposed on many of our members as a result of the overlapping jurisdiction of other financial regulators enforcing their own Gramm-Leach-Bliley Act ("GLB Act") information security program rules or guidelines ("Safeguards Standards"). There will be many circumstances where entities will be subject to overlapping requirements of more than one set of Safeguards Standards. A FFELP participant could be subject to the Commission's rule, and at the same time share customer information with an affiliate or service provider that is subject to the Safeguards Standards of another GLB Act regulator. In this case, the affiliate or service provider could be subject to two sets of requirements. An example would be a bank that serves as a custodian or a lockbox for a nonprofit entity serving as a FFELP lender. Similarly, a FFELP participant subject to the Commission's

jurisdiction could receive customer information as an affiliate or service provider of an entity subject to jurisdiction of another GLB Act regulator. This organization could also be subject to overlapping requirements. An example would be a bank that uses a loan servicer to administer its student loan portfolio. There is a very real possibility of confusion in these cases.

The Commission notes in the preamble to the proposed rule that, in the case of affiliates of entities subject to the Commission's rule that are covered by another agency's Safeguards Standards, it does not intend to duplicate the existing requirements on the affiliate. We believe this principle should be expanded to also apply in the case of service providers subject to another agency's Safeguards Standards. We also believe the principle should be applied in reverse. Specifically, we believe that entities subject to the Commission's jurisdiction that comply with the Commission's Safeguards Standard should not have to worry about compliance with a (slightly) different Safeguards Standard of another GLB Act regulator because they are affiliates or contractors of entities subject to the jurisdiction of such other regulator.

We believe there is a simple way to resolve the problem. We recommend that, with respect to affiliates and service providers of entities subject to a GLB Act regulator, each regulator deem the affiliate or service provider to be in compliance with the regulator's Safeguards Standards if the affiliate or service provider is in compliance with the Safeguards Standards of its direct functional regulator. Acceptable assurance of such compliance should be a representation from such affiliate or service provider that such entity is in compliance with the Safeguards Standards of its GLB Act regulator, together with an annual certification of continued compliance. We note that this approach would also apply in cases where the financial institution and its affiliate or service provider were subject to the jurisdiction of the same functional regulator (e.g. the Commission). Since the Commission's proposed rule follows substantially the same format as that of the other GLB Act regulators, we believe this approach satisfies the consumer protection objectives of the GLB Act. We recognize that this approach will require the Commission to coordinate its activities with your sister agencies, and may require those agencies to issue amendatory guidance. Nonetheless, we believe this approach represents a workable solution that advances the objectives of the GLB Act, and relieves financial institutions of the burden and uncertainty involved in compliance with the duplicative or varied rules of more than one regulator. It also should simplify the enforcement responsibilities of the federal regulatory agencies.

In addition, we offer the following comments in response to other sections of the proposed rule:

1. The Commission notes that the proposed rule only addressees safeguards pertaining to "customer information". See proposed section 314.1. Though we recognize that some financial institutions retain personal financial information on individuals who do not meet the definition of customer, we believe the Commission's reading of the scope of its statutory mandate is correct. We also

agree that, as a practical matter, the safeguards developed by a financial institution will cover all personal financial information retained by the institution simply because institutions generally do not segregate information on customers separately from information on others.

2. The Commission asks for comment on the benefits and burdens of the requirement set forth in proposed section 314.3(a) that a financial institution have a written information security program. We believe that this requirement is reasonable, both because of the Commission's general "flexible" approach and because the proposed rule specifically does not require the information to be in a single document. The proposed rule simply requires that "all parts of the program are coordinated and can be identified and accessed readily." This approach should not be unduly burdensome for smaller entities because it accounts for the "size and complexity of the entity, and the nature and scope of its activities" while still providing a "comprehensive coordinated approach to security." For these reasons, we support the proposed requirement as written.

3. The Commission requests comment on the proposed rule that requires each financial institution to designate an employee or employees to coordinate its information security program. See proposed rule 314.4(a). We can accept this proposal. Though this rule imposes a specific requirement, it provides financial institutions organizational flexibility in determining how to best structure its information security program. We encourage the Commission to retain unchanged the proposal to allow a financial institution to designate an appropriate employee(s) to develop and implement its information security program or create a working group or committee for this purpose. Further, we concur with the Commission's position in not mirroring the Banking Agency guidelines requiring board of director involvement. As noted, some organizations subject to the FTC's jurisdiction do not have a board of directors. The Commission's rule also is consistent with standard business practice by putting this important task in the hands of those with the necessary expertise.

4. The Commission requests comment on the benefits and burdens of requiring a financial institution's risk assessment to include coverage of prescribed areas of operation. See proposed rule 314.4(b). The Commission's Rule should not prescribe specific operational areas for risk assessment, but should, consistent with the Banking Agency Guidelines, require risk assessment in those areas of operation that management deems relevant for that particular institution (i.e., based on the institution's size, organizational structure, business lines and the sensitivity of the customer information involved). We believe that individual financial institutions are in the best position to identify specific operational areas within their particular organizational structure that are relevant to assessing risks to information security. Mandating risk assessment in predefined operational areas could hamper management's ability to act, and deploy appropriate resources, in the manner that most effectively assesses risk at that particular institution. A financial institution should not be forced to conduct risk assessment

in areas of operation that may not be appropriate for the institution, and shouldn't face compliance uncertainty if its operational structure does not neatly reflect the core areas of operation specifically set forth in the proposed rule. Further, service providers subject to both the Commission's Rule and the Banking Agency guidelines (which do not identify specific areas of possible risk) should not face inconsistent requirements or be forced to expend unwarranted resources to satisfy both sets of requirements. In fact, it is conceivable that some entities could be faced with complying with even a third set of Safeguard Standards (such as those of the SEC).

5. The Commission requests comments on the requirement that financial institutions regularly test or otherwise monitor key controls, systems and procedures, and comment specifically on the fact that specific audits or test are not required. See proposed rule 314.4(c). We support the Commission's proposed rule as written, which gives management discretion to determine the audit procedures or tests, and testing timeframes, for monitoring the effectiveness of the financial institution's safeguards. We concur that each institution should have the flexibility to adopt procedures that best reflect business and risk management practices appropriate to the institution's size, organizational structure, and business lines.

   Flexibility in testing requirements will only add to the effectiveness of these tests. The design of firewall protection is illustrative; it must by necessity adapt rapidly as predators discover new methods of breaching security and different operating environments will have different security methods. On the latter point, for example, UNIX and Windows NT operating systems each have different ways of defining security. Within the education lending community, the need for flexible testing requirements is also driven by the customary exchange of loan data among multiple trading partners. The many participants in the FFELP - lenders, guarantors, schools, secondary markets, origination and disbursement agents, and the Department of Education - all have unique data security protocols and should be permitted to develop equally unique security testing configurations.

6. The Commission requests comment on whether it is necessary for financial institutions to enter into contracts requiring service providers to maintain appropriate safeguards for protecting customer information, or whether equally effective alternatives exist. We believe the proposed rule set forth in proposed section 314.4(d), if modified as recommended in the next paragraph, represents the appropriate approach. The selection of service providers customarily involves the use of contractual provisions to restrict the information practices of service providers and to impose responsibilities for employing proper information protections. Except as proposed in the next paragraph, the final rule should continue to allow financial institutions to utilize contracts to ensure that service providers maintain appropriate safeguards and take appropriate steps when weaknesses are detected.

   The Commission requests comment on whether the final rule should offer an

exception to the contract requirement for service providers that are financial institutions or are subject to other Safeguards Standards. We believe that such an exception should be made in the case of financial institutions subject to the Safeguards Standards of the Commission or another GLB Act regulator. As explained in our opening comments, we believe that, for these financial institutions, a representation that they are in compliance with the Safeguards Standards of their functional regulator should either replace the requirements of proposed section 314.4(d) or be recognized as a way to satisfy the requirements. As recommended previously, we believe it would be reasonable to expect that this representation be kept up-to-date with an annual certification of compliance by the entity with the Safeguards Standards of its functional regulator.

The Commission further requests comment on whether additional guidance is needed on what safeguards are appropriate for service providers. The addition of more detailed guidance would create an inconsistency with the Banking Agency guidelines, since those guidelines do not list specific or unique safeguards applicable to servicer providers. These inconsistencies would be particularly burdensome for entities that have affiliates subject to the Commission's rule and others subject to the Banking Agency guidelines. The Commission's rule should ensure uniformity with the guidelines and generally require service providers to maintain appropriate safeguards without prescribing what processes and procedures meet that general requirement. Service providers are best equipped to determine appropriate safeguards in light of their size, scale, organizational structure, and the sensitivity of the customer information they handle, and also in light of contractual arrangements with financial institutions.

7. The Commission requests comment on the requirement set forth in proposed section 314.4(e) that each financial institution evaluate and adjust its information security program in light of material changes to its business that may affect the safeguards. We support the requirement as proposed. Specifically, we recommend the Commission maintain the brevity and flexibility of this provision by retaining its current wording. Specifically designated systems and procedures may become obsolete as technology and business practices evolve, resulting in useless safeguards being implemented to meet the form of the regulation, while leaving new areas of risk unguarded. Identifying specific items now would require frequent regulatory changes that might, again, leave certain newly developed areas unprotected. This provision appropriately places the responsibility to keep an institution's information security program up-to-date and effective.

8. The Commission also requests comment on the appropriate amount of time for covered entities to comply with the Commission's final rule. The proposed rule states that the final rule will be effective one year from the date of its issuance. See proposed section 314.5. While a one-year period is probably sufficient for all entities to comply with the final rule, we strongly believe the period should not

be shortened. In this regard, we note that many different types of entities are subject to the Commission's rule. Certainly, most FFELP institutions have effective information security processes in place. However, organizations will need to reassess their current processes in light of the final, formal requirements, and to develop or enhance existing processes to comply with the more structured infrastructure, processes, and documentation requirements included in the Commission's rule. In addition, a few entities may be unaccustomed to the process by which a formal information security program is developed, implemented, and maintained. For these entities, we believe that at least one year will be needed to formalize these steps.

The one qualification in this area relates to any requirement that would entail amending existing agreements with service providers. We note in this regard that the Banking Agencies gave entities subject to their jurisdiction 29 months to accomplish this task. We recommend that a similar period be granted to entities subject to the Commission's jurisdiction. Specifically, we would suggest that any requirement to open up existing contracts not become effective until 2 1/2 years following publication of a final rule.

9. You also ask for comment on how to address possible overlap with other laws and rules pertaining to information security. We addressed the issue of overlap with the Safeguards Standards issued by the other GLB Act regulators in our opening comments. Other laws and regulations relating to information security raise a different set of questions. Unlike the case of the other Safeguards Standards, these provisions may not be substantially similar to the Commission's safeguards rule. For this reason, we believe that the Commission should review on a case-by-case basis whether compliance with such other laws or rules should be deemed to constitute compliance with the Commission's safeguard rule.

We appreciate the opportunity to comment on the proposed rule. If you have any questions, please contact us at the number listed below.

Sincerely,

Mark Powden
President
Education Finance Council
1155 15th Street, N.W.
Washington, D.C. 20005
Phone: 202-466-8621

Sheldon Repp
General Counsel
National Council of Higher Education Loan Programs
1100 Connecticut Ave., N.W.
Washington, D.C. 20036
Phone: 202-822-2106