

Nancy L. Perkins
Nancy_Perkins@aporter.com
202.942.5065
202.942.5999 Fax
555 Twelfth Street, NW
Washington, DC 20004-1206

October 9, 2001

Secretary
Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

**Re: Gramm-Leach-Bliley Act Privacy Safeguards Rule
16 CFR Part 314 - Comment**

Dear Secretary:

On behalf of the National Association of Mutual Insurance Companies ("NAMIC"), we respectfully submit the comments below to the Federal Trade Commission ("the Commission") on its proposed Standards for Safeguarding Customer Information ("proposed Rule") published in the Federal Register on August 7, 2001.¹

NAMIC is a full-service national trade association with more than 1,200 member companies that underwrite 40 percent (\$123.3 billion) of the property/casualty insurance premiums in the United States. NAMIC's membership includes five of the ten largest property/casualty carriers, every size regional and national property/casualty insurer and hundreds of farm mutual insurance companies. All of NAMIC's member companies are "financial institutions," within the meaning of the Gramm-Leach-Bliley ("GLB") Act of 1999, and thus are subject to the law's requirement to protect the security and confidentiality of their customers' nonpublic personal information.²

As insurance companies, NAMIC's members are subject to the GLB Act's privacy and security requirements as implemented by the state insurance regulators. However, particularly because most of the state insurance regulators are still in the process of formulating their security standards, the Commission's Rule is a model for regulation of NAMIC's members.³ Indeed, under Section 504 of the GLB Act, the state

¹ 66 Fed. Reg. 41,162 (proposed Aug. 7, 2001) (to be codified at 16 C.F.R. Part 314).

² 15 U.S.C. § 6801(a).

³ Only one of the states, New York, has completed its drafting of the required security standards. See N.Y. Regulation No. 173 (draft) (to be codified at N.Y. Comp. Codes R. & Regs. tit. 11, § 421).

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 2

insurance authorities are required to consult and coordinate with the Commission and the other federal agencies charged with prescribing privacy and security regulations under the GLB Act, "for the purposes of assuring, to the extent possible, that the regulations prescribed by each such agency and authority are consistent and comparable with the regulations prescribed by the other such agencies and authorities."⁴ Thus, NAMIC and its members have a significant stake in the outcome of the Commission's Rule.

In our comments below, the references to "FR" are to the Federal Register version of the proposed Rule. References to "the Preamble" are to the introductory commentary accompanying the proposed Rule. Specific proposed standards are identified by the sections of chapter 16 of the Code of Federal Regulations in which they would be codified.

A. Purpose and Scope (proposed Section 314.1)

Section 314.1 of the proposed Rule describes the purpose and scope of the security standards. In discussing this section, the Preamble provides a clarification of the Commission's intent that is not readily evident from the proposed Rule itself: that the Rule cover "not only financial institutions that collect information from their own customers, but also financial institutions that receive customer information from other financial institutions."⁵ The Commission has requested comment on this point.

We believe, consistent with certain of the comments previously submitted to the Commission,⁶ that it would be highly inappropriate to impose on financial institutions obligations respecting the security of information on customers of other financial institutions. The reasons for our position are both legal and practical. First, we respectfully disagree with the conclusion that imposing such obligations "is within the authority conferred by the [GLB] Act."⁷ Title V, Subtitle A of the GLB Act ("Subtitle A") expressly states Congress' intent with respect to the privacy protections it prescribes:

⁴ 15 U.S.C. § 6804(a)(2). As the Commission is aware, the National Association of Insurance Commissioners is facilitating coordination among the state insurance regulators by preparing model legislation/regulations for GLB Act implementation purposes.

⁵ FR at 41,164.

⁶ See *id.*, n.24.

⁷ FR at 41,164.

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 3

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of *its* customers and to protect the security and confidentiality of *those* customers' nonpublic personal information.⁸

It is clear from this statement that Congress intended that the security standards to be promulgated under Subtitle A apply to each financial institution with respect to information it receives on *its own* customers, and *only those* customers. There is no suggestion in the statute or its legislative history that Congress intended to subject financial institutions to any of the Subtitle A privacy or security requirements with respect to nonpublic personal information they may receive on customers of other financial institutions. Indeed, the Commission's proposal in this regard appears starkly inconsistent with congressional intent.

Second, as a practical matter, we believe the proposed extension of the Rule to information received on other institutions' customers would be extremely difficult, if not impossible, to administer. We envision particular problems for financial institutions such as credit reporting companies and the Insurance Services Office that regularly receive large quantities of information from insurance companies, including information on third-party claimants, i.e., persons who are not policyholders of the insurer providing the information. In order to comply with the Rule as proposed, these and other financial institutions would have to determine, in every instance in which they receive information on an individual: (1) whether the information is "nonpublic personal information" within the meaning of the GLB Act and its implementing regulations (which may require a search of publicly available information (lists, etc.)); (2) whether the source of the information is a "financial institution" within the meaning of the GLB Act and its implementing regulations; and (3) if the source is a financial institution, whether the person to whom the information pertains is a "customer" (not merely a "consumer") of that financial institution within the meaning of the GLB Act and its implementing regulations. Undertaking this analysis with respect to all personal information received from any source (as well as, of course, applying the required safeguards to all information thereby appearing to be "customer information") would subject financial institutions to a vastly overburdening endeavor – one that, as explained above, Congress appears never to have intended them to have to undertake.

⁸ GLB Act, § 501(a), 15 U.S.C. § 6801(a) (emphasis added).

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 4

We therefore strongly urge that the Commission withdraw its proposal to require financial institutions to abide by the Rule with respect to information on customers of other financial institutions.

B. Definitions (proposed Section 314.2)

1. Customer Information

Proposed Section 314.2(b) defines “customer information,” as:

[A]ny record containing nonpublic personal information, as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

We believe this proposed definition is unduly broad. First, we object to the inclusion of the word “handled” in the proposed definition. This word is not included in the definition of customer information in the GLB Act security standards promulgated by the federal banking agencies.⁹ We believe the inclusion of the word “handled” is unwarranted and would create serious confusion and ambiguity regarding the application of the Rule. The requirements for ensuring the security of customer information involve technologies and systems that a financial institution may reasonably and effectively monitor and control. Applying such technologies and systems to information “maintained” by the institution, as is required both by the Commission’s proposed Rule and the banking agencies’ security standards, appears generally feasible. However, applying those technologies and systems to any customer information “handled” by the institution does not. It is not clear, for example, whether information on a customer that is conveyed to the financial institution orally would be deemed to be information “handled” by the institution. Nor is it clear whether information sent by electronic mail to the institution but not retained by the institution would be deemed “handled” by the institution. These examples are merely suggestive of the potential problems that including the word “handled” in the definition of “customer information” would create.

⁹ See 12 C.F.R. Part 30, App. B (Office of the Comptroller of the Currency); 12 C.F.R. Part 208, App. D-2 and 12 C.F.R. Part 225, App. F (Federal Reserve System); 12 C.F.R. Part 364, App. B (Federal Deposit Insurance Corporation); 12 C.F.R. Part 570, App. B (Office of Thrift Supervision) [hereinafter “Interagency Guidelines”].

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 5

We also believe that limiting the “customer information” definition to information that a financial institution maintains will effectively ensure the security and confidentiality protection Congress sought to provide under Subtitle A.

Second, we object to the inclusion of the words “or your affiliates” in the proposed definition of “customer information.” Here too, the Commission is deviating – and very significantly – from the standards adopted by the federal banking agencies. Each of the banking agencies’ standards apply, respectively, to information on customers that is maintained by or on behalf of a regulated institution – not also to information maintained by or on behalf of such institution’s affiliates.

As the Commission appears to recognize in its commentary on this issue, the extension of the Rule to information on customers that is handled or maintained “by or on behalf of affiliates” could pose substantial burdens on entities subject to other agencies’ or authorities’ security standards and create significant confusion and ambiguity regarding the proper safeguards to apply.¹⁰ Moreover, the Commission’s proposal would, we believe, exceed the authorized scope of the Rule by effectively subjecting to the Commission’s regulation financial institution affiliates that are not within Commission jurisdiction.

The Preamble states that the Commission has proposed to cover information handled or maintained by or on behalf of affiliates for the following reason:

[T]o ensure that customer information does not lose its protections merely because it is shared with affiliates, which is freely allowed under the G-L-B Act and Privacy Rule.¹¹

This explanation itself suggests that the proposed “affiliate” extension of the “customer information” definition is beyond the authorized scope of the Rule. Congress carefully considered and deliberately decided against prescribing in the GLB Act any new privacy or security standards with respect to affiliate information-sharing by financial institutions. Instead, Congress expressly reconfirmed in Subtitle A the existing affiliate information-sharing rules set forth in the Fair Credit Reporting Act.¹² Although Congress may in the

¹⁰ See FR at 41,165.

¹¹ Id. at 41,164.

¹² See 15 U.S.C. § 6806.

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 6

future revisit the issue through new legislation, the Commission's current mandate is to implement Section 501(b) of the GLB Act and not any possibly anticipated or desired new legislation.

We respect the Commission's stated intent not to duplicate existing requirements for affiliates that are financial institutions directly subject to safeguards standards.¹³ In principle, we also sympathize with the Commission's concern about the confidentiality of information shared by financial institutions with affiliates that either are not financial institutions or are not required to safeguard information about other financial institution's customers.¹⁴ However, we believe the proposed Rule inappropriately deals with these issues: it fails to address the problem of potentially conflicting or otherwise inconsistent information security standards, and, as discussed above, it reaches beyond the authority prescribed by the GLB Act (and any other statute) with respect to the Commission's regulatory jurisdiction.

Even if there were no jurisdictional problem with the proposed affiliate-sharing aspect of the "customer information" definition, we would object to it on grounds of practicality and fairness. According to the Preamble, under the proposed definition:

[T]o the extent that a financial institution shares customer information with its affiliates, the proposed rule would require it to ensure that the affiliates maintain appropriate safeguards for the customer information at issue.¹⁵

Apparently, the Commission intends that each financial institution serve as a "watchdog" over each and every affiliate with whom it shares information about a customer of its own or any other financial institution. Under the Rule as proposed, a failure to effectively ensure, through such policing of affiliate practices, an affiliate's security compliance will trigger GLB Act penalties for the institution itself. We find this proposal unduly burdensome, inherently unworkable, and fundamentally unsound. Imposing on a financial institution the obligation to monitor and discipline the practices of its affiliates, of which there may be an increasing number in light of the expanded

¹³ See FR 41,165.

¹⁴ See *id.*

¹⁵ *Id.* at 41,164.

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 7

types of affiliations authorized by the GLB Act, is wholly inappropriate, particularly in light of the distinct regulatory regimes governing such affiliates.

In short, we strongly object to including any reference to affiliates in the Rule's definition of "customer information."

2. *Information Security Program*

Proposed Section 314.2(c) defines "information security program" as:

[T]he administration, technical, or physical safeguards you use to access, collect, process, store, use, transit, dispose of, or otherwise handle customer information.

We object to this proposed definition for essentially the same reasons that we object to the definitions discussed above: it is unnecessarily overbroad and is inconsistent with the definition of the parallel term "customer information systems" in the federal banking agencies' security standards. Specifically, we object to the inclusion in the "information security program" definition the term "process" and the phrase "or otherwise handle" – neither of which are part of the banking agencies' "customer information systems" definition. Although this inconsistency with the banking agencies standards is subtle, it has important practical significance: as discussed above, the term "handle" is inherently ambiguous, and the term "process" also could cause interpretive problems. Because the Rule will require the application of an institution's security safeguards to any customer information with respect to which the institution takes any of the actions referenced in the "information security program" definition, we believe the definition should be tailored carefully to conform to the banking agencies' standards and must be clear, straightforward, and permit reasonably manageable implementation of the required safeguards.

C. *Elements (proposed Section 314.4)*

1. *Designation of Coordinating Employee(s)*

Paragraph (a) of proposed Section 314.4 requires each financial institution, as part of its design of an information security program, to designate an employee or employees to coordinate the program. We agree with the comments previously submitted to the Commission explaining that it would be inappropriate for the Rule to require the

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 8

involvement of a financial institution's Board of Directors in oversight of the information security program.¹⁶ We agree that financial institutions need flexibility determining how best to ensure supervision of their information security programs, including management and oversight by appropriate employees.

2. Risk Assessment

Paragraph (b) of Section 314.4 requires each financial institution to identify, for purposes of its information security program, foreseeable risks that could result in the "unauthorized disclosure, misuse, alteration, destruction, or other compromise" of customer information. We note that while this requirement generally parallels the banking agencies' security standards, the banking agencies' standards do not include the phrase "or other compromise" in their corresponding provision.¹⁷ We suggest that, in order to conform the Rule more closely to the banking agencies' standards, as required by Congress,¹⁸ and to prevent confusion, the Commission omit from the final Rule the reference to "or other compromise." This phrase is sufficiently broad and ambiguous to pose interpretation and implementation problems for financial institutions, in contrast to the relatively straightforward terms "disclosure," "misuse," "alteration" and "destruction."

3. Oversight of Service Providers

Paragraph (d) of proposed Section 314.4 requires each financial institution to oversee its service providers, including by entering into a contract with each such provider requiring the provider to implement and maintain information safeguards in accordance with the Rule. The Commission has requested comment on this proposed requirement, particularly with respect to the benefits and burdens of the required contracts.¹⁹

We believe that financial institutions should not be required in all instances to enter into contracts binding their service providers to adhere to the Rule's security safeguards. As the Commission has noted, some service providers may themselves be

¹⁶ See FR at 41,166 & n.42.

¹⁷ See Interagency Guidelines, *supra* note 9.

¹⁸ 15 U.S.C. § 6804(a)(2).

¹⁹ FR 41,166.

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 9

financial institutions or be subject to other safeguards standards, and some service providers may receive customer information under the general exceptions set forth in sections 313.14 and 313.15 of the GLB Act Privacy Rule.²⁰ As the Commission suggests, in order to account for these circumstances, it would make sense for the Rule to provide exceptions from the contract requirement for certain service providers. We therefore support the Commission's suggestion that, if any contract requirement is to be included in the final version of Section 314.4, there be exceptions to that requirement for service providers that either (1) are themselves financial institutions, (2) are subject to other safeguards standards, or (3) receive information pursuant to section 313.14 or section 313.15 of the GLB Act Privacy Rule.

In addition, if the Commission determines that the final Rule should contain any requirement for a contract with service providers as part of Section 314.4, we would strongly urge it to clarify that financial institutions will not be held liable under the Rule for breaches of such a contract by a service provider absent some knowing involvement by the financial institution. We perceive significant harm in any possible interpretation of the Rule that would subject a financial institution to potential liability for actions of its service providers that the institution neither precipitated, participated in or otherwise endorsed or effectuated.

D. Effective Date (proposed Section 314.5)

Proposed Section 314.5 requires each financial institution to implement an information security program within one year from the date of issuance of the final Rule. The Commission has requested comment on (1) whether one year is an appropriate time period for institutions to implement such programs and (2) whether the Rule should include a "grandfathering" provision, similar to the provision in section 313.18(c) of the GLB Act Privacy Rule, to allow the continuation of existing contracts with service providers even if they may not satisfy the Rule's requirements.

We believe the proposed one-year implementation period is too short to enable financial institutions to prepare for compliance with the Rule. In order to meet the objectives of Congress and the Commission with respect to customer information security – i.e., to (1) ensure the security and confidentiality of the information, (2) protect against threats or hazards to such security and the information's integrity, and (3) protect against unauthorized and potentially harmful access to or use of the information –

²⁰ *Id.*

ARNOLD & PORTER

Secretary
Federal Trade Commission
October 9, 2001
Page 10

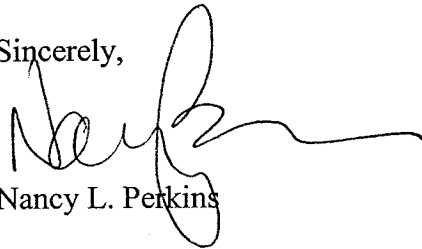
financial institutions will have to undertake comprehensive systems development, installation, and testing. In addition, financial institutions will need to design and test their systems to ensure proper coordination and monitoring of the service providers with whom they share customer information. Particularly for larger and more compartmentalized institutions, completing these steps in an effective and responsible manner will almost certainly require more than one year. We therefore believe the Rule should provide a minimum of two years for implementation of the required information security program.

With respect to existing contracts with service providers, we strongly endorse the Commission's suggestion that the Rule include a grandfathering provision for such agreements, along the lines of the GLB Act Privacy Rule. We note that the banking agencies' security standards also contain such a grandfathering provision,²¹ and we believe the Commission's Rule should be consistent with those standards in this respect. To ensure such consistency in substance as well as intent, we note that the Commission's Rule would need to provide for the grandfathering of any contract with a service provider entered into on or before a date that is at least 30 days after the date of publication of the final Rule in the Federal Register.

* * *

We appreciate the opportunity to comment on the Commission's proposed Rule. If you have any questions regarding our comments, please contact me either by phone at (202) 942-5065 or by fax at (202) 942-5999, or by e-mail to perkina@aporter.com.

Sincerely,



Nancy L. Perkins

²¹ See Interagency Guidelines, *supra* note 9.