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

Comments of the National Independent Automobile Dealers Association Directed to The Federal Trade Commission, Washington, D.C. 20580.

Section A. Background.

The Federal Trade Commission ("FTC") is required to establish the Safeguards Rule for financial institutions under its jurisdiction pursuant to Section 501(b) of the Gramm-Leach-Bliley Act (the "Act"). Section 509(3)(A) of the Act contains the definition of the term "financial institution". A financial institution is defined as "any institution the business of which is engaging in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956." In the FTC's Final Rule on Privacy of Consumer Financial Information ("Privacy Rule"), 16 CFR Part 313, the FTC chose to retain a broad definition of "financial institution". That definition encompasses retail sellers of goods if they assist purchasers in obtaining credit or extend credit themselves. In certain circumstances, the FTC's Privacy Rule may apply to motor vehicle dealerships. Those dealerships would also be subject to the Financial Institutions Safeguards Standards adopted by the FTC.

The National Independent Automobile Dealers Association (NIADA) has represented independent motor vehicle dealers for over 50 years. The National Association and its State Affiliate Associations represent more than 15,000 independent motor vehicle dealers located throughout the United States. In the year 2000, the sale of used motor vehicles generated more than $363 billion in revenues. Approximately 41.6 million used motor vehicles were sold in the United States with used motor vehicle sales representing 70 percent of all motor vehicle sales. Because vehicles are lasting longer (the average vehicle on the road today is 8.5 years old), projections of future used vehicle sale volumes suggest that the used vehicle market will maintain its 40 million-plus volume in the years to come.[1] Given the number of motor vehicle transactions that take place each year, the Safeguards Rule will have a significant impact on the used retail motor vehicle industry.

On September 7, 2000, the FTC published a Notice and Request for Comment on developing the administrative, technical, and physical information Safeguards Rule. The comments were originally due on October 10, 2000, but the time to submit comments was extended for an additional fourteen (14) days pursuant to a subsequent notice published by the FTC. NIADA submitted comments in response to the Notice and Request for Comments published by the FTC and a final recommendation that the FTC Safeguards Rule adopt a "reasonable policies and procedures" standard and related guidelines rather than specific rules. After considering the comments submitted by a variety of parties, the FTC published the Proposed Rule and a Notice and Request for Comment in August of 2001. Comments must be submitted by October 9, 2001. NIADA hereby submits its comments with respect to the same.

Section B. Overview of Comments Submitted.

In the Comments NIADA submitted in October 2000, NIADA urged the FTC to adopt a flexible "reasonable policies and procedures" standard for safeguarding information and related guidelines rather than specific requirements. The proposed Safeguards Rule provides that each information security program should be appropriate to the size and complexity of the financial institution, the nature and scope of its activities, and the sensitivity of the customer information at issue. At the same time, consistent with the Banking Agency Guidelines, the proposed Rule requires that certain basic elements that the Commission believes are important to information security be included in each program. In order to develop, implement and maintain an information security

---

[1] The 2001 Used Car Market Report, Manheim Auctions, 1400 Lake Hearn Drive NE, Atlanta, GA 30319.

program, each financial institution must: 1) designate an employee or employees to coordinate its program; 2) assess internal and external risks to its security, confidentiality and integrity of customer information in each area of its operations; 3) design and implement an information security program to control these risks; 4) require service providers (by contract) to implement appropriate safeguards for the customer information at issue; and 5) adapt its program in light of material changes to its business that may affect its safeguards. NIADA commends the FTC for following the general approach of the Banking Agency Guidelines and proposing flexible requirements wherever feasible. The focus of NIADA's Comments is (1) on modifying the definitions and provisions governing and the scope of information and entities covered in the Safeguards Rule to ensure that they are consistent with those used in the Act and the Privacy Rule and (2) including additional guidelines to enhance the ability of financial institutions to comply with the Safeguards Rule.

Section C. Section-by-Section Analysis.

1. Proposed §314.1: Purpose and Scope.

a. The handling of customer information by financial institutions that collect and receive customer information.

The FTC has requested comments regarding the benefits and burdens of and/or other issues or concerns that should be considered if the FTC imposes the requirements of the Proposed Safeguards Rule on all financial institutions that collect information from their own customers, as well as financial institutions that receive customer information from other financial institutions. In the Comments submitted on October 24, 2000, NIADA agreed that the Safeguards Rule should apply with respect to financial institutions that receive nonpublic personal information from another financial institution, whether it is an affiliate or nonaffiliated third party. NIADA believes this position is within the authority conferred upon the FTC by the Act and is consistent with Section 502(e) of the Act and Section 313.11 of the FTC's Privacy of Consumer Financial Information, both of which address the "Limits on Redisclosure and Reuse of Information".

Section 502(e) of the Act provides that:

> A nonaffiliated third party that receives nonpublic personal information from a financial institution shall not, directly or indirectly through an affiliate, disclose the information to any person that is not affiliated with both the financial institution and the third party, unless the disclosure would be lawful if made directly by the financial institution.

The FTC's Privacy Rule also imposes limits on redisclosure and reuse of information. The provisions in Section 313.11 of the Privacy Rule apply both to a nonaffiliated third party that receives information from a financial institution and the third party's affiliates.[2] In sum, the entity that receives the information will "step into the shoes" of the financial institution that made the initial disclosures. The recipient party's ability to disclose information will be limited based upon the circumstances under which the information was obtained by the original financial institution. If the information is provided pursuant to an exception, the recipient may disclose information to its affiliates and affiliates of the financial institution that provided the information pursuant to an exception. For information received outside an exception, it may disclose the information pursuant to an exception and in accordance with the opt out and privacy notice given by the financial institution making the initial disclosures.[3] If a recipient party is subject to the FTC's jurisdiction and it is entitled to receive, reuse and redisclose information provided by a financial institution in accordance with the Act and Privacy Rule, NIADA believes the recipient financial institution should also be required to comply with the FTC's Safeguards Rule. Including the financial institutions that collect information as well as those that receive customer information will provide greater safeguards for both the financial institutions and their customers.

---

[2] 33666 Federal Register/Vol.65, No. 101 Wednesday, May 24, 2000/Rules and Regulations/Section 313.11.

[3] Id.

b. Compliance with Alternative Standards.

NIADA agrees with the commenters that urged that compliance with alternative standards should constitute compliance with the Safeguards Rule, whether it is the SEC Rule, the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance and Accountability Act ("HIPAA") of 1996 or other Federal Consumer Protection Statutes, such as the Fair Credit Reporting Act ("FCRA") and the Equal Credit Opportunity Act ("ECOA"). Motor vehicle dealerships must comply with a number of records retention requirements specified in over 900 federal and state regulations, including requirements to maintain credit related documents, sales and lease contracts, statements regarding cash proceeds, and various other documents related to the transaction, for a period of time extending anywhere from two to six years.[4]

For example, two of the documents that may be obtained by a motor vehicle dealer when a purchaser requests an extension of credit to fund the transaction include a credit application and a credit report, if the dealership obtains credit reports. The FCRA and ECOA already impose a number of duties upon credit reporting agencies and any users of a credit report to protect the confidentiality and integrity of that information. Motor vehicle dealers are prohibited from disclosing personally identifiable information contained in the application unless the customer consents in writing to the disclosure and the dealer has a "permissible purpose" for obtaining credit information about the customer and certifies that the report will not be used for any other purpose. The customer has a right to receive a notice indicating whether or not credit has been approved and, if it is denied, additional information as to the reason for denial and a free disclosure of the consumer's file from a credit reporting agency. Likewise, if a person denies credit based either wholly or partly upon information from a person other than a credit reporting agency and the information is the type of consumer information covered by the FCRA, the FCRA requires the user to disclose to the consumer his or her right to obtain disclosure of the nature of the information that was relied upon by making a written request. Any dispute as to the accuracy of the information relied upon must be investigated, the source of the information must review the evidence and report findings to the credit reporting agency, and the consumer is entitled to receive a written report regarding the investigation and a copy of the report if the investigation results in any change. Any inaccurate or unverified information must be removed or corrected. If the investigation does not resolve the dispute, the consumer may add a statement to his or her file regarding the dispute that will then be included in future reports.

The FCRA also imposes certain obligations on companies that share information with entities related by common ownership or affiliated by corporate control. Information obtained from outside sources may be shared among affiliates only after notice to the consumer giving the consumer the opportunity to direct that such information not be communicated. Absent this notice, the information may be considered a consumer report under the Act. Failure to comply with the FCRA can result in state or federal enforcement actions, as well as private lawsuits. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution.

A number of other Acts under the FTC's jurisdiction likewise include a duty to provide full disclosure to the consumer; obtain affirmative consent that the information contained in the document is true and accurately reflects the transaction with the consumer; retain records of the transaction; and protect the integrity of the information provided, including: the Truth in Lending Act/Regulation Z and Truth in Leasing Act/ Regulation M (copies of disclosure statements); the Federal Odometer Act (odometer disclosure statements); the FTC Used Car Rule (copies of buyers' guides) and the Magnuson-Moss Warranty Act (copies of limited warranty and service contract documents). In each case, the records are often open for reasonable inspection by the state department of motor vehicles as well as other federal and state agencies. To the extent that a financial institution or recipient of information is required to maintain and protect the integrity of records pursuant to other laws, they too would be liable for any damage caused to the consumer for the unauthorized release of that information and, therefore, compliance with these laws should constitute compliance with the FTC's Safeguards Rule.

---

[4] Guide to Record Retention Requirements, G.P.O., Washington, D.C. 20402

2. Proposed Section 314.2: Definitions.

The Definition Section defines terms for purposes of the Safeguards Rule. Unless otherwise stated, the terms used in the Safeguards Rule bear the same meaning as in the Privacy Rule. The proposed Safeguards Rule contains three "new" terms: "customer information", "information security program;" and "service provider". To the extent that the FTC feels these additional terms are necessary, they should be consistent with the terms used in the Privacy Rule. The FTC should not expand the scope of covered information or the persons or entities subject to the Rule by adopting broader definitions.

a. Proposed Section 314.2(b): Customer Information.

Proposed Section 314.2(b) defines "customer information" as "any record containing nonpublic personal information, defined in 16 CFR 313(n) of the Privacy Rule, 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." The definition of "customer information" should be consistent with the definition of "nonpublic personal information" as defined in the FTC's Final Privacy Rule. The FTC has recognized that the plain language of Section 501 warrants limiting the Safeguards Rule to "customer information", but the proposed definition may be interpreted as expanding the scope of covered information by adopting a new definition for "customer information". In order to be consistent in its interpretation, the FTC should clarify that "customer information" only refers to those records that contain "(i) Personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."[5] Retail sellers of goods may compile lists of customers from sources other than in connection with providing financial products and services. For example, motor vehicle titles are public records. They contain the name of the selling dealer along with the name and address of the purchaser of a vehicle. If a list is derived using such information, it does not contain "customer information" because it was not compiled using personally identifiable financial information (i.e. it was not obtained in connection with providing a financial product or service to the customer). In sum, in order to avoid additional confusion, NIADA proposes that the FTC clarify that the definition of "customer information" is analogous to the definition of nonpublic personal information as defined in 16 CFR 313(n).

The FTC further explained that its proposed Rule would include information "handled or maintained" by or on behalf of a financial institution and its affiliates so that customer information does not lose its protections merely because it is shared with affiliates, which is freely allowed under the Act and Privacy Rule. However, the language used by the FTC may be overly broad to accomplish the stated objective and beyond the authority granted to the FTC. For instance, a motor vehicle dealership may store paper and/or electronic copies of its records at a different offsite location where the information will only be stored, not utilized by, the facility. A storage facility is not a "financial institution" or an "affiliate", yet it may be subject to the FTC's Safeguards Rule because it is "handling or maintaining" records that contain nonpublic personal information about a customer of a financial institution. Given that nonaffiliated third parties and affiliates of a financial institution are subject to the FTC's Privacy Rules and the Limits on Redisclosure and Reuse of Information in Section 313.11 therein, NIADA believes that, to the extent that a financial institution shares customer information with these entities and they are otherwise subject to the FTC's Privacy Rules, the information they obtain should be safeguarded in accordance with the Safeguards Rule. Yet not every entity that "handles or maintains" a record containing nonpublic personal information should be subject to the jurisdiction of the FTC. NIADA recommends that the definition be modified to clearly state that customer information includes nonpublic personal information as defined in 16 CFR 313(n) that is collected and maintained by a financial institution or its affiliates.

b. Proposed Section 314.2(d): Service Provider

The definition of "service provider" in the Safeguards Rule should be consistent with the definition in the Act and the FTC's Privacy Rule. Section 502(b) of the Act and Section 313.13 of the

---

[5] FTC Final Privacy Rule Section 313.3(n)(1)(i) and (ii).

Privacy Rule create an exception to certain notice and opt out requirements for "service providers and joint marketing". The service provider/joint marketing exception applies whenever a financial institution provides nonpublic personal information to *a nonaffiliated third party to perform services for it or on its behalf*, including the marketing of the financial institution's own products or services or financial products or services offered pursuant to a joint agreement between two or more financial institutions. As proposed in the Safeguards Rule, "Service Provider" is defined as "*any person or entity* that receives, maintains, processes, or otherwise is permitted access to customer information *through its provision of services* directly to a financial institution that is subject to the rule." (Emphasis added). This definition is much broader than the definition used in the Act and Privacy Rule and, in turn, would require a number of individuals and entities not otherwise covered by the Act and Privacy Rule to comply with the Safeguards Rule. The definitions utilized in the Act, Privacy Rule and Safeguards Rule, whenever possible, should be consistent and bear the same meaning so as to avoid confusion. The FTC should also refrain from establishing safeguards that apply to persons or entities not otherwise subject to its jurisdiction. The proposed definition of service provider, therefore, should be modified to refer to any nonaffiliated third party that performs services for or on behalf of a financial institution and receives, maintains, processes or otherwise is permitted access to customer information in order to perform those services.

Furthermore, the FTC's Safeguards Rule should not apply to all nonaffiliated third party service providers given that the Privacy Rule does not require financial institutions to enter into confidentiality contracts with service providers that receive information under the general exceptions in Sections 313.14 and 313.15 of the Privacy Rule. Sections 313.14 and 313.15 specifically state that the requirements for service providers and joint marketing in Section 313.13 do not apply if the financial institution discloses nonpublic personal information for one of the purposes set forth in those Sections. That having been said, NIADA recognizes that any nonaffiliated financial institution that receives nonpublic personal information under an exception in Sections 313.14 and 313.15 is subject to the Limits on Redisclosure and Reuse of Information contained in Section 313.11 and, therefore, it may be in the interest of both the disclosing and recipient party to insert a confidentiality provision in the contractual agreement, if one exists. Whether the financial institution chooses to do so, however, should be at its own discretion and should be part of its risk assessment and the implementation of the information safeguards it deems appropriate to protect both itself and its customers.

3. Proposed Section 314.3: Standards for Safeguarding Customer Information and Proposed Section 314.4: Elements.

NIADA appreciates the difficulty of the FTC's task in establishing and implementing appropriate safeguards standards for the wide range of financial institutions subject to its jurisdiction and supports the objectives of the Act and the FTC's Safeguards Rule as articulated in Section 501(b) and Section 314.3(b) respectively. NIADA commends the FTC for providing general standards and flexibility to implement the safeguards appropriate to meet the goals of the Safeguards Rule while taking into consideration each financial institution's size, the nature and scope of its activities, the sensitivity of the customer information at issue, the standard practices in the industry and the specific experiences of that entity. At the same time, NIADA believes that the costs and burdens of complying with the Safeguards Rule may be reduced and the benefits afforded to customers enhanced by including additional guidelines to assist the financial institutions to develop, implement and maintain the information security program, as well as examples of mechanisms or policies and procedures that the FTC would consider reasonable.

a. Proposed Sections 314.4(b) and (c): Identifying Risks and Implementing Safeguards

Section 314.4 sets forth general elements that a financial institution "shall" develop, implement and maintain as part of its information security program. Subsection (b) requires a financial institution to identify internal and external risks to the security, confidentiality and integrity of customer information and assess the sufficiency of any safeguards in place to control the risks. Subsection (c) then requires the financial institution to design and implement information safeguards to control the risks it identified through the risk assessment and to regularly test and monitor the effectiveness of the safeguards' systems and procedures. While the Rule identifies some risks

that should be considered, neither subsection offers guidance as to the types of risks that should be considered and/or the measures that may be appropriate to safeguard against the risks identified. NIADA agrees that it should ultimately be up to the financial institution to identify and assess "reasonably foreseeable risks" that may threaten the security or integrity of customer information and to develop "reasonable policies and procedures" to protect against those threats and hazards, but the FTC should issue guidelines on how to identify and safeguard against potential risks, similar to Section III of the Final Interagency Guidelines. In Section III.C.1 of the Interagency Guidelines, the Agencies identified eleven factors an institution should consider in evaluating the adequacy of its policies and procedures to effectively manage risks. Although implementation of the factors is not mandatory, they offer financial institutions guidance as to the types of factors they should be considering.

b. Proposed Section 314.4(a): Designation of Employee or Employees

NIADA also has concern regarding the implications raised by Section 314.4(a), which requires a financial institution to designate an employee or employees to coordinate an information security program. The institution, not an individual within the institution, is responsible for complying with the Safeguards Rule. If individual employees are designated as being responsible for the development of the security program, in the event a problem does arise, a customer may attempt to impute individual liability upon those employees so appointed. The financial institution should have the discretion to determine who within the organization should carry out responsibilities under the security program and, so long as it is able to develop, implement and maintain written information security program in accordance with the FTC's Safeguards Rule, it should not be required to specifically designate any individual employee(s) as being responsible for the security program.

c. Proposed Section 314.4(d): Service Providers

NIADA supports the general purpose of requiring service providers to comply with the Safeguards Rule and recognizes that it is necessary to protect the security and confidentiality of the information disclosed. However, as the FTC recognized when it adopted the Privacy Rule, there is a limit to the measures a financial institution can take to protect the information that it provides. Section 313.13 of the FTC's Privacy Rule provides that a customer does not have the right to opt out of having nonpublic personal information disclosed to nonaffiliated third parties if the financial institution provides the initial notice in accordance with Section 313.4 of the Privacy Rule and enters into a contract with the third party that prohibits the third party from disclosing or using this information other than to carry out the purposes for which it was disclosed, including use under an exception in Section 313.14 or 313.15 in the ordinary course of business to carry out those purposes. The FTC concluded, and NIADA agrees, that the protections set out in the statute are adequate for purposes of the Privacy Rule.[6]

For the most part, NIADA believes the obligations imposed by the Safeguards Rule are consistent with the requirements set forth in Section 502(b) of the Act and Section 313.13 of the FTC's Privacy Rule. Proposed Section 314.4(d) of the Safeguards Rule requires a financial institution to oversee service providers by:

(1) selecting and retaining service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) requiring your service providers by contract to implement and maintain such safeguards.

With respect to Section 314.4(d)(1), NIADA proposes that the FTC clarify that financial institutions must use initial due diligence that reflects each institution's business structure and complexity and ensures initial compliance by third parties with appropriate protection standards. For example, the financial institution may take into consideration whether a service provider is subject to the FTC's Safeguards Rule, or another federal or state law that imposes a duty to protect customer information consistent with the FTC's Safeguards Rule, and the degree of sensitivity of the information to which the third party provider has access during the due diligence

---

[6] 33670 Federal Register/Vol. 65, No. 101/Wednesday, May 24, 2000/Rules and Regulations/Section 313.13

process. After taking this information into account, each institution could be expected to include appropriate provisions in its service provider contracts to promote the protection of customer information.

Although NIADA supports requiring service providers to implement and maintain appropriate safeguards by contract, NIADA is opposed to any requirement that would impose an obligation upon the financial institution to continuously "oversee" and "monitor" service providers' compliance with the FTC's Safeguards Rule. The language stating that a financial institution must "oversee" service providers, when read in conjunction with the language in subparagraph (1), could be interpreted as imposing an obligation upon the financial institution to "monitor" or "ensure" compliance by a service provider with the FTC's Privacy Rule and Safeguards Rule. NIADA asserts that such an obligation would be impossible to satisfy. Moreover, if a financial institution provides customer information and records to another person or entity, that person/entity is responsible for knowing its obligations under applicable law, including the FTC's Safeguards Rule, and the financial institution should not be responsible for monitoring its compliance therewith. This interpretation is consistent with the FTC's Comments in the Privacy Rule.

The FTC stated in the Comments to Section 313.11 of the Final Privacy Rule that "The final rule does not impose a general duty on financial institutions to monitor third parties' use of nonpublic personal information provided by the institutions...Also, the limits on reuse as stated in the final rule provide a basis for an action to be brought against an entity that violates those limits." The FTC further stated, and NIADA agrees, however, that if the financial institution imposes a limitation on what the recipient may do with the information it provides, it may have a duty to ensure that the recipient party acts in accordance with that contract. NIADA maintains that this can be done effectively by including contractual provisions that give the financial institution the right to receive copies of self-audits and the service provider's records and, if the financial institution deems it necessary based upon the due diligence process, the right to audit the records and practices of the service provider to ensure that the service provider implements information security measures that are consistent with the contractual agreement.

The FTC expressed in the Privacy Rules its belief that a balance must be struck that minimizes interference with existing contracts while preventing evasions of the regulations.[7] The imposition of an oversight or monitoring standard for service providers would create a standard that many financial institutions will be unable to meet. Motor vehicle dealerships may have numerous locations and service providers and it would be nearly impossible to monitor whether every lender, financial institution, mail house and third-party vendor is complying with the Safeguards Rule. From a service provider's prospective, it could be subject to continuous audits of its information creating constant interruption of its normal business operations and jeopardizing the security of other records and information retained by the service provider. Therefore, the balance in this case is best struck by imposing an obligation upon the financial institution to use due diligence in selecting service providers and entering into appropriate contractual arrangements whereby the service provider is required to implement appropriate measures to meet the objectives of the Safeguards Rule, while holding the service provider responsible for complying with its contractual obligations and the Safeguards Rule.

4. Potential Impact on Small Entities.

NIADA believes that most, if not all, financial institutions will have to retain the services of consultants to advise them of their responsibilities under the Act and the FTC's Privacy and Safeguards Rules; assess threats to customer information; develop, implement and test security programs to address potential risks; assist with due diligence in selecting service providers and draft appropriate language for contracts with service providers; and create the written security program. The actual costs and burdens associated with developing a comprehensive information security program in written form will vary from institution to institution depending upon a number of variables, including: The type of business conducted; the size of the institution; the number of affiliated and nonaffiliated parties with which it shares information; the number of employees; and the policies and procedures it has in place to comply with other laws and regulations that impose consumer protection and record retention requirements. In any case, the cost of complying will be

[7] 33670 Federal Register/Vol. 65, No. 101/Wednesday, May 24, 2000/Rules and Regulations/Section 313.13.

significant. In the case of smaller financial institutions, there are fewer employees with the expertise to provide instruction on compliance with new regulatory obligations.

To the extent the Safeguards Rule contains gray areas or lacks clarity, the costs and burdens associated with compliance increase while the benefits of having such protection for customers decrease. NIADA recognizes that the FTC does not have the authority to exempt small businesses from complying with the Safeguards Rule, but it does have the ability to include definitions and obligations consistent with those imposed by the Act and Privacy Rule and to provide additional guidance on factors that an institution should consider when assessing risks and developing reasonable policies and procedures to protect customer information. While these measures will not eliminate the burdens and costs small businesses will have to incur, they will help keep them to a minimum.

5. Proposed Section 314.5: Effective Date.

NIADA agrees that a year from the date on which a Final Safeguards Rule is issued is probably adequate time for most financial institutions to implement an information security program, but requests that the FTC consider providing an eighteen month period for implementation to afford additional time to test security programs and ensure that appropriate safeguard measures have been established. As for the contractual obligations with service providers, NIADA requests that the Rule contain a transition period to allow the continuation of existing contracts with service providers, even if they would not satisfy the Rule's requirements, for a period of two-years for all contracts entered into on or before the effective date of the Final Safeguards Rule. This "two-year grandfathering of service agreements" provision would be consistent with the grandfathering clause in the FTC's Final Privacy Rule.

Section D. Conclusion.

NIADA appreciates the FTC's decision to provide financial institutions with latitude to assess the risks that threaten the integrity and confidentiality of customer information, to develop "reasonable policies and procedures", and to modify those policies and procedures as necessary to meet the goals of the Act and the FTC's Safeguards Rules. The FTC should, however, include guidelines to assist financial institutions to assess the risks that may threaten the security, integrity and confidentiality of customer information, as well as examples of mechanisms or policies and procedures that the FTC would consider reasonable to minimize those risks. Furthermore, whenever possible, the definitions and the provisions governing the scope of information and entities covered in the Act and the FTC's Privacy and Safeguards Rules should be consistent. Additional guidelines and consistent application of definitions will help minimize the burdens and costs of complying with the Safeguards Rule while increasing the likelihood that customer information is adequately protected.

NIADA would like to thank the FTC for the opportunity to comment with respect to the proposed Safeguards Rule. Any questions the FTC has regarding NIADA's comments and the position taken herein may be directed to NIADA's Legal Counsel, Keith E. Whann or Deanna L. Stockamp, of the law firm Whann & Associates located at 6300 Frantz Road, Dublin, Ohio 43017.