

Gramm-Leach-Bliley Act Privacy Safeguards Rule
16 CFR Part 3__-Comment



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

Section A. Background

On September 7, 2000, the Federal Trade Commission ("FTC") published a Notice and Request for Comment on developing the administrative, technical, and physical information Safeguards Rule. The 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"). 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.

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 across the United States. In 1998, the sale of used motor vehicles generated more than \$338 billion in revenues. Approximately 40 million used motor vehicles were sold and used motor vehicle sales represented 72 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 could have a significant impact on the used retail motor vehicle industry. Therefore, NIADA is submitting 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.

Section B. Questions as to Scope of the Commission's Safeguards Rule.

1. Range of Information Subject to the Safeguards Rule.

The FTC has requested comments regarding the range of information that should be subject to the Safeguards Rule. In its Final Privacy Rule, the FTC determined that the required disclosures and the timing of those disclosures depends upon whether a financial institution has established a "consumer relationship" or "customer relationship", thereby acknowledging that Congress did not intend to use "consumer" and "customer" interchangeably. In order to be consistent in its interpretation, that distinction should apply equally to Section 501 of the Act which refers solely to "customers' nonpublic personal information" and "customer records and information", which we interpret to be the same. In other words, "customer records and information" refers to those records and/or information related to the "nonpublic personal information" obtained by a financial institution that enters into a consumer relationship which is continuous in nature. This term does not cover records and information related to business customers or consumers who have not established an ongoing relationship with a financial institution. If the intent of Congress is to

¹ 1999 Used Car Market Report, ADT Automotive, Inc., 435 Metroplex Drive, Nashville, Tennessee 3721.

apply the Safeguards Rules to all information and records obtained, consumer and customer, it would not have made a distinction.

Furthermore, the information and records governed by the Safeguards Rule should not include records and information that is already adequately protected by other federal and state laws. 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 Fair Credit Reporting Act already imposes a duty upon credit reporting agencies and any users of a credit report to protect the confidentiality and integrity of that information.

2. Range of Financial Institutions Subject to the Safeguards Rule.

The FTC also requested comment on the range of financial institutions to which the Safeguards Rule should apply. Given that the language in Section 502(b) refers to “customer’ nonpublic personal information” and “customer records and information”, only those financial institutions that establish a consumer relationship that is continuous in nature and obtain “nonpublic personal information” as defined under the FTC’s Privacy Rule should be required to comply with the Safeguards Rule. Furthermore, NIADA proposes that only one financial institution, the entity that ultimately owns or services the loan, should be required to comply with any specific Safeguards requirements. The FTC has already recognized that it is appropriate to consider a loan transaction as giving rise to only one customer relationship and that the customer relationship may be transferred in connection with a sale or transfer of the loan or servicing rights. Often when a loan is sold or transferred to another financial institution, the customer records and information are also transferred to that institution. Therefore, just as the initial financial institution is relieved from its obligation to make annual disclosures regarding its privacy policies when it “terminates” the customer relationship, it should also be relieved of the obligation to maintain the records and information in accordance with the Safeguards Rules. At the same time, if a financial institution discloses customer records and information to a financial institution that has no customer relationships or consumers, the party receiving the information should be required to comply with the Safeguards Rule in its handling of the information provided by the originating financial institution.

NIADA does recognize that there may be instances when information should be protected even if it is obtained by a financial institution that establishes a consumer relationship or a short term customer relationship. However, the records and information obtained in those instances are typically protected by other state and federal laws and regulations. For instance, 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 daily sales summaries, for a period of time extending anywhere from two to six years.² In fact, a number of Acts under the FTC’s jurisdiction include a duty to retain records, including: the Equal Credit Opportunity Act (copies of credit applications, supplemental information used in evaluating applicants, and written notifications); 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) and the Used Car Rule (buyers’ guides, sales contracts, and related warranty or service contract documents). In each case, the records are stored and maintained by the dealership in a secure location to which only authorized personnel have access. Those records are often open for reasonable inspection by the state department of motor vehicles as well as other federal and state agencies.

²Guide to Record Retention Requirements, G.P.O., Washington, D.C. 20402.

Section C. Questions as to Other Aspects of the Commission's Safeguards Rule.

1. Small Financial Institutions and 2. Specificity of the Safeguards Rule.

NIADA appreciates the difficulty of the task imposed upon the FTC in establishing and implementing appropriate safeguards standards for the wide range of financial institutions subject to its jurisdiction. Given the variation in size and complexity of the financial institutions governed by the FTC's Final Privacy Rule, the nature and scope of their activities and the information they collect, and the nature of their respective resources, NIADA believes it is virtually impossible for the FTC to develop standardized rules or procedures for every entity subject to its jurisdiction. For instance, in the motor vehicle industry there is an enormous disparity in the size of dealerships. Some dealers operate single locations and others operate multi-locations. They also differ vastly with respect to the number of motor vehicles they sell, the amount of records they generate, how they retain records (i.e. by filing hard copies or storing computer files), and the systems to which they have access. In addition, the records and information a motor vehicle dealership obtains from a purchaser depends upon the type of financing transaction involved (i.e. sale or lease, traditional, subprime, or buy here-pay here). With the enactment of the Electronic Signatures in Global and National Commerce Act, issues related to completing a transaction and record retention will probably become even more complicated. The FTC should not expect entities that vary so vastly in size and business practices to implement and comply with the same safeguards standards.

Furthermore, as this is a Rule that will be applied nationally, uniformity should be one of the foremost considerations of the FTC. Implementation of uniform laws and rules is an underlying principal that has led to the rewrite of Articles in the Uniform Commercial Code and enactment of legislation such as the Electronic Signatures in Global and National Commerce Act. Therefore, rather than specifying particular security measures that must be adopted in order to comply with the FTC's Safeguards Rule, the FTC should require financial institutions to develop "reasonable policies and procedures" that are designed to meet the goals of the Act and the FTC's Privacy Rule. The FTC should include guidelines to assist the financial institutions to assess the risks that may threaten the security, integrity and confidentiality of consumer and customer information, as well as examples of mechanisms or policies and procedures that the FTC would consider reasonable to minimize those risks and meet the goals of the Act and FTC Rules. The actual compliance mechanisms implemented by each financial institution will vary from institution to institution depending upon the size of the institution, the amount and type of records and information obtained, its access to more efficient and cost effective safeguard mechanisms, and other policies and procedures it has in place to comply with other laws and regulations that impose disclosure, non-disclosure, and retention requirements.

Utilizing a general standard as proposed by NIADA will allow the FTC to establish a more thorough and consistent standard that applies to every financial institution. It will avoid overly burdensome, costly, and impractical standards from being imposed upon smaller institutions and will create less confusion about how to comply with the Act and the FTC Privacy and Safeguards Rules. Establishing a more general "reasonable policies and procedures" standard is also consistent with standards adopted in other state and federal statutes. For example, most state statutes include what is commonly referred to as a "Bona Fide Error Defense". The Bona Fide Error Defense allows a supplier to avoid paying certain damages if an error occurs when the supplier can demonstrate that it occurred "notwithstanding procedures reasonably adopted to avoid the error". The reasonableness of the procedures may be impacted by the standard practices in the industry and the specific experiences of that entity. The same consideration should be given to financial institutions that are required to implement safeguards for customer records and information. Many financial institutions, including most motor vehicle dealerships, may already have adequate mechanisms in place to protect that information.

3. Statutory Objectives.

a. Anticipation of Threats or Hazards to Security or Integrity.

Section 501(b) requires the Commission to establish standards for administrative, technical and physical safeguards to "protect against anticipated threats or hazards to the security or integrity" of customer records and information obtained by financial institutions. The FTC requested comments on whether and how "anticipated threats and hazards" should be defined. NIADA takes the position that the FTC should issue guidelines on how to identify potential threats and hazards, but it should ultimately be up to the financial institution to identify and assess the 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. The anticipated threats or hazards to the security of customer records will vary greatly among the institutions. For instance, a small independent motor vehicle dealership may store its records at the dealership where only two employees have potential access to the information. On the other hand, a larger, multi-location dealership may employ several people who have access to customer records and information by virtue of their employment duties, and it may have records stored at a different location offsite or via a complex computer system with file sharing capabilities. Therefore, specifying anticipated threats and hazards in the Rule would be inappropriate. With respect to requiring that the financial institution reassess the threats or hazards at certain intervals or upon the occurrence of specific events, those issues should also be left to the discretion of the financial institution and would be relevant as to whether it has developed "reasonable" policies and procedures.

Finally, NIADA does not believe it is practical to grant customers periodic access to their records in order to monitor the accuracy of the information. First, this requirement could have a substantial and costly impact on financial institutions, many of which store their records elsewhere and have to pay for their retrieval. Second, it would also jeopardize the security of other records and information retained by the financial institution by providing more people with access to the records than would otherwise be necessary. Third, in many cases the records and information, such as that obtained by a motor vehicle dealership, is included in documents which the purchaser must review and sign, thereby acknowledging that they contain true and accurate information. The dealership is then required to provide the purchaser with copies of all signed documents and the dealership personnel are prohibited by law from revising or modifying the documents or the information contained therein.

b. Preventing Unwarranted Access and Use.

In addition to requiring protection against anticipated threats and hazards, Section 501(b) requires that the safeguards standards "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." §501(b)(3). The FTC indicated that "unauthorized access" and "unauthorized use" are not defined and requested comments on whether the terms should be defined and, if so, how. NIADA interprets "unauthorized access" and "unauthorized use" to mean that safeguard standards should be in place to prevent any persons or entities from having access to or use of the information unless they are acting as an authorized agent or representative of the financial institution, or are a person or entity that must receive the records or information to accomplish that which the customer has given the financial institution permission to do. In other words, if a purchaser requests that a motor vehicle dealership assist the purchaser to obtain financing from a lender, the purchaser has authorized the dealership to allow its authorized personnel to have access to and use of the customers credit information and records, and has authorized the dealership to submit that information to other lending institutions and their authorized personnel for the purpose of obtaining credit.

NIADA believes that due to the diverse range of financial institutions subject to the FTC's jurisdiction, it is not practical to develop uniform minimum procedures to protect against unauthorized access or use of information. It should be up to the financial institution to identify

and assess the potential for unauthorized access or use of customer records or information and to develop "reasonable policies and procedures" to protect the records and information. The FTC should include guidelines regarding how to implement "reasonable polices", which may include using confidentiality agreements with employees, training employees in procedures for preventing unauthorized access to and use of customer records and information, distributing employee manuals explaining safeguard procedures, and establishing access rights to customer information. Ultimately, it should be up to the financial institution to identify and assess the risk of unauthorized access or use of records and to develop "reasonable policies and procedures" to prevent others from accessing the information.

An issue which the FTC did not request comment upon, but which NIADA believes should be addressed in the Safeguards Rule, is the definition of "substantial harm or inconvenience to any customer." Taking steps necessary to obtain a copy of a loan document, verification of a debt, or a credit report certainly should not constitute a "substantial harm" or "substantial inconvenience". But at what point does a harm or inconvenience become "substantial?" The Rule should include examples of what does and does not constitute "substantial harm or inconvenience" to a customer.

c. Insuring Security and Confidentiality.

Section 501(b) also requires that the safeguards standards "insure the security and confidentiality of customer records and information." §501(b)(1). This requirement does not mean anything more than protecting against "anticipated threats or hazards" or "unauthorized access and use". The same policies and procedures that protect against threats and hazards and unauthorized access and use will insure security and confidentiality. Furthermore, if the initial financial institution provides customer information and records to another financial institution, or any other entity for that matter, that institution is responsible for knowing its obligations under applicable law, including the FTC's Rules, and the initial financial institution should not be required to notify the recipient of the limitations on reuse and redisclosure of the information.

Section D. Consideration of Other Agencies' Safeguards Standards.

Section 505 of the Act contains the Enforcement provisions. Section 505(b)(1) states that the agencies and authorities described in subsection (a), with the exception of those set forth in Section 501(b)(2), shall implement the standards prescribed under Section 501(b) as standards prescribed pursuant to Section 39(a) of the Federal Deposit Insurance Act. Section 505(b)(1) governs the Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Federal Reserve Board (FRB), and Federal Deposit Insurance Corporation (FDIC), among other agencies and authorities. On June 26, 2000, the OCC, OTS, FRB and FDIC published proposed Guidelines establishing standards for safeguarding customer information. As proposed, the Interagency Guidelines provide that each financial institution should develop its own safeguards policies and procedures and the Guidelines do not specify particular security measures that must be adopted.

In Section 505(b)(2), the agencies and authorities described in paragraphs (3), (4), (5), (6), and (7) of subsection (a) shall implement the standards prescribed under Section 501(b) "by rule". Section 505(b)(2) encompasses agencies and authorities such as the Securities and Exchange Commission (SEC) and the FTC, among others. On June 22, 2000, the Securities and Exchange Commission (SEC) adopted a final Safeguards Rule as part of its Privacy of Consumer Financial Information Final Rule. The SEC's Safeguards Rule restates the objectives of Section 501(b) and passes along to financial institutions the requirement to develop policies and procedures that are "reasonably designed" to meet the goals of the Act. NIADA does not interpret the Act as requiring more specific requirements than those set forth in the SEC's Rule, nor does it believe that the Act's requirement that the SEC and FTC issue a rule rather than guidelines warrants a different approach than that taken by the Interagency Guidelines and the SEC.

E. Conclusion.

The FTC Safeguards Rule, like the Interagency Guidelines and the SEC Rule, should include guidelines to assist financial institutions to assess the risks that may threaten the security, integrity and confidentiality of consumer and customer information, as well as examples of mechanisms or policies and procedures that the FTC would consider reasonable to minimize those risks and meet the goals of the Act and FTC Safeguards Rule. It should ultimately be up to the financial institution 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 Privacy and Safeguards Rules.

Given the broad definition of financial institutions, it would be almost impossible to adopt specific uniform standards without imposing substantial costs and hardships upon a number of the institutions. In addition, as in the case of the motor vehicle industry, the additional costs and hardships that would result from imposing specific safeguards requirements would provide little, if any, benefits to their consumers or customers.

The "nonpublic personal information" a motor vehicle dealership may obtain when extending credit or assisting a purchaser to obtain credit from a lender includes a credit application, a credit report, and other documents related to the purchaser's credit history and ability to pay. Motor vehicle dealerships already have policies and procedures in place to protect the safety, integrity and confidentiality of the documents and information collected. Once a person decides to negotiate the purchase of a motor vehicle, he is referred to the dealership's F&I Department. The F&I personnel have been trained regarding how to complete credit applications, make the appropriate disclosures to the purchaser regarding the use of the information, obtain permission to submit the credit information to lenders, and protect the confidentiality of the documents and information that is submitted to and received from the lenders. By agreement with the lenders, the dealership is usually required to provide a list of the employees who may transmit and receive information regarding the purchaser's request for credit and the dealership is liable for any misuse of the records and information.

Furthermore, the purchaser must review and sign the sale or lease contract and all of the documents related to the purchase or lease of a vehicle, thereby acknowledging that they contain true and accurate information. The dealership is then required to provide the purchaser with copies of all of the signed documents and the dealership personnel are prohibited by law and by company policy from revising or modifying the documents or the information contained therein. Upon completion of the transaction, the original records are often transferred to the financial institution that extends the credit or services the loan. To the extent required by applicable law, originals or copies of the records and information are retained by the dealership in a secure location and/or computer system to which only management and authorized personnel have access. When the loan or lease is paid in full and/or when the applicable retention period expires, the records are disposed of in a manner that preserves the safety and confidentiality of the information contained in the records.

In sum, NIADA believes that most motor vehicle dealerships already have developed effective safeguards policies and procedures in order to comply with federal and state record retention requirements and as part of the policies and procedures they have in place to prevent errors from occurring in their day to day operations. To the extent they have not established adequate safeguards for the nonpublic personal information they obtain, NIADA is confident that they have the ability and means to do so.

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.