WHANN & ASSOCIATES, LLC
ATTORNEYS AT LAW

KEITH E. WHANN
DEANNA L. STOCKAMP
JAY F. MCKIRAHAN
of Counsel

6300 FRANTZ ROAD
DUBLIN, OHIO 43017
(614) 764-7440
FAX (614) 764-0091

MEMORANDUM

TO: MICHAEL LINN, NIADA EXECUTIVE VICE PRESIDENT

FROM: KEITH E. WHANN AND DEANNA L. STOCKAMP

DATE: APRIL 29, 2003

RE: COMPLIANCE WITH THE FEDERAL TRADE COMMISSION'S SAFEGUARDS RULE

Most dealers are familiar with the requirements of the Gramm-Leach-Bliley Act and the Federal Trade Commission's (FTC) Privacy Rule, which obligate them to create and distribute Privacy Notices to their customers. What they may not know is that the FTC's Standards for Safeguarding Customer Information, more commonly known as the "Safeguards Rule," becomes effective on May 23, 2003. The objectives of the Safeguards Rule are to insure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security and integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

The FTC's Safeguards Rule does not change the dealership's obligations under the FTC's Privacy Rule. The Privacy Rule deals with how financial institutions collect and share information. Motor vehicle dealerships are still required to provide their customers with a Privacy Notice that advises the customer about the types of information the dealership collects, the sources from which the information may be obtained and the dealership's policies with respect to sharing that information. As you may recall, in order to fully comply with the Gramm-Leach-Bliley Act and the FTC's Privacy Rule, motor vehicle dealers were also required to make a statement about their information safeguarding practices in their Privacy Notices. As a result, most dealership Privacy Notices state "we maintain physical, electronic and procedural safeguards to protect the confidentiality and security of the information we collect". Now the Safeguards Rule mandates that dealers have a written document that specifies the steps they have taken to assess the types of risks that exist with respect to the information being obtained by unauthorized individuals and to protect the confidentiality and security of such information.

Like the Privacy Rule, the Safeguards Rule applies only to transactions involving persons who obtain a financial product or service from the dealership primarily for personal, family or household purposes. Although it is a good idea to apply the same privacy policies and information security standards to all of the information collected by the dealership, it is not required for information about companies or individuals who obtain financial products or services for business, commercial or agricultural purposes, unless the dealership's Privacy Notice states otherwise. Personal information typically collected from customers at the dealership includes their names, addresses, telephone numbers, birth dates and social security numbers, information contained in credit applications and credit reports, information dealerships receive from lenders, and even lists of the dealership's finance customers.

The FTC's Safeguards Rule specifically requires every dealer, regardless of the size of his dealership, to develop, implement and maintain a comprehensive written information security plan that describes the dealership's program to protect customer information. It also requires them to ensure that affiliates of the dealership maintain appropriate safeguards and that their service providers are capable of maintaining appropriate safeguards for the customer information the dealership shares. The Dealership's written information security plan must: (1) Designate an employee or employees to coordinate the safeguards; (2) Identify and assess the risks to customer information in each relevant area of the dealership's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) Design and implement a safeguards program, and regularly monitor and test it; (4) Select appropriate service providers and contract with them to implement safeguards; and (5) Evaluate and adjust the program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring of safeguards.

When we filed comments regarding the Safeguards Rule on behalf of NIADA, we requested that the FTC adopt flexible requirements, and the FTC did just that. The dealership's privacy policies and information security standards must be developed taking into consideration the dealership's size and complexity, the nature and scope of its activities, the sensitivity of the information it collects, and theses policies and standards must be regularly monitored. When implementing the Safeguards Rule, the dealership must consider all areas of its operation, including three that are particularly important to information security: Employee management and training; information systems, and managing system failures. In an effort to help businesses understand and comply with the FTC's Financial Information Safeguards Rule, the FTC issued a new "Facts for Business" Publication titled "Financial Institutions and Customer Data: Complying with the Safeguards Rule."

While compliance with the FTC's Safeguards Rule is just around the corner and, therefore, on the top of everyone's agenda, dealers are well advised to consider other Federal Privacy and Anti-Terrorism Laws that have recently been enacted or are under consideration. For example, on October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act). Title III of the USA Patriot Act makes a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act (BSA) that are intended to promote the prevention, detection, and prosecution of international money laundering and the financing of terrorism. Under the USA Patriot Act, the term "financial institution" is defined to include a "business engaged in vehicle sales, including automobile, airplane, and boat sales."

The Treasury Department has already issued a Final Rule implementing Section 314 of the USA Patriot Act, which establishes procedures that encourage information sharing between governmental authorities and financial institutions, and among financial institutions themselves. The first part of the Rule establishes a mechanism for law enforcement agencies to communicate the names of suspected terrorists and money launders to financial institutions in an effort to locate and secure accounts and transactions involving those suspects. Effective as of September 26, 2002, any motor vehicle dealerships that receive the name of a suspect must designate one person at the dealership to be the contact person regarding the request and any future requests that it receives. They must also establish adequate procedures to protect the security and confidentiality of the requests received from FinCEN and their responses to these requests. The requirement to maintain adequate security and confidentiality procedures to protect the information is met if the dealership applies the same procedures it has established to comply with the Gramm-Leach-Bliley Act and the FTC's Safeguards Rule.

The USA Patriot Act also requires every financial institution to establish an anti-money laundering program. Pursuant to Section 352 of the Act, the anti-money laundering program must include, at a minimum: (1) The development of internal policies, procedures, and controls; (2) The designation of a compliance officer; (3) An ongoing employee-training program; and (4) An independent audit function to test programs. Section 326 of the Act further requires the Treasury to prescribe Regulations setting forth minimum standards for financial institutions to identify customers applying to open accounts, including: (1) Adopting reasonable procedures for verifying the identity of any person seeking to open an account; (2) Maintaining records of the information used to verify the person's identity, including the person's name, address, and other identifying information; and (3) Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by a Government Agency. Although motor vehicle dealers have been temporarily exempted from the requirement to establish an anti-money laundering compliance program, on February 24, 2003, FinCEN published an Advance Notice of Proposed Rulemaking to solicit public comments as to how these requirements should apply to motor vehicle dealers.

To eliminate the need for NIADA Members to draft new or modified privacy policies and information security standards in the future, we have developed the enclosed materials to assist them in complying not only with the FTC's Safeguards Rule, but also with the USA Patriot Act and emerging implementing regulations that will impact every dealership's policies, practices and overall operations. These materials are being provided to you for distribution to NIADA Members free of charge. We are also providing them to you in electronic format to make it easy for dealers to customize them for their own use. Enclosed you will find the:

FTC Guidelines titled "Financial Institutions and Customer Data: Complying with the Safeguards Rule," which summarize the purpose for the Safeguards Rule and include suggested policies and procedures for complying with the Rule.

Program Coordinator's Audit of Dealership Privacy Policies and Information Security Standards Checklist

Dealership Privacy Policies and Information Security Standards

Employee Agreement to Comply with Privacy Policies and Information Security Standards

Statement of Privacy Policies and Information Security Standards

Addendum to Service Provider Agreements and Letter to Service Providers Regarding Safeguarding Information

Please keep in mind that these materials are designed to assist dealers to identify and implement appropriate policies and standards for protecting customer information. They are intended as a guide for motor vehicle dealers to develop their privacy policies and information security standards. While not intended as a universal solution that every dealership can adopt, since they are drafted from a used motor vehicle dealer's perspective, NIADA Members should find that they are easy to use and customize for their dealerships. It is important that dealers be instructed to familiarize themselves will all of the information contained in the documents provided and include only those privacy policies and information security standards that are feasible for the dealership to implement and maintain. In addition, there may be state specific data protection or safeguards rules with which dealers must comply and, therefore, they may wish to consult with their legal counsel or other professional consultants to ensure that their

privacy policies and information security standards are appropriate for the dealership and in compliance with applicable federal and state laws, rules and regulations. The information contained in this document and the additional materials provided are for general information purposes only and should not be considered as legal advice.