NATIONAL AUTOMOBILE DEALERS ASSOCIATION
8400 Westpark Drive • McLean, Virginia 22102
703/821-7040 • 703/821-7041

Legal & Regulatory Group

September 18, 2006

Via E-Mail

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex M)
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Re: The Red Flags Rule
Project No. R611019

Dear Secretary:

The National Automobile Dealers Association (NADA) submits the following comments in response to the joint notice of proposed rulemaking (JNPR) issued by the Federal Trade Commission (FTC), the federal banking agencies, and the National Credit Union Administration (the agencies) to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[1]

NADA represents approximately 20,000 franchised dealers in all 50 states and the District of Columbia who sell new and used vehicles and engage in service, repair, and parts sales. NADA's members include over 2,300 franchised dealers who sell medium- and/or heavy-duty trucks. Our members collectively employ well in excess of 1 million people nationwide. A significant number of our members are small businesses as defined by the Small Business Administration. Accordingly, NADA is particularly focused on regulatory changes that will increase the regulatory burden on small businesses.

NADA supports the anti-identity theft goals set forth in the FACT Act and the JNPR and the agencies' stated desire to adopt a flexible, risk-based approach that is appropriate to the size and complexity of the regulated entity and the nature and scope of its activities. Because automobile and truck dealers typically assume the risk of loss in finance and lease transactions involving identity theft, they already have a business incentive to develop and implement practical procedures to help prevent this crime. However, as discussed below, we are concerned that the JNPR proposes requirements that are: (i) beyond the scope of the statutory mandate; (ii) unlikely

[1] Unless otherwise indicated, these comments refer to the portion of the JNPR applicable to section 114.

to achieve the anti-identity theft goals of the statute; (iii) ambiguous; and (iv) exceedingly burdensome.

Consistency with Statutory Mandate

Section 114 of the FACT Act generally requires the agencies to establish and maintain *guidelines* for regulated entities to use regarding identity theft, to prescribe regulations requiring regulated entities to establish reasonable policies and procedures for implementing those guidelines, and to identify patterns, practices, and specific forms of activity indicating the possible existence of identity theft. Senate Report 108-166 explains these requirement, in part, as follows:

> The Committee intends for the guidelines to provide flexibility to institutions given the changing nature of identity theft and related crimes. The Committee expects that the guidelines adopted will vary based on a number of factors, including the size and sophistication of the institution. The Committee does not believe that a 'one size fits all' approach is appropriate — *the guidelines should be a general outline* for use by financial institutions, creditors, and other users of consumer reports…. Although institutions and others must establish reasonable policies and procedures to identify possible risks to consumer accounts, the Committee again notes that such policies and procedures will vary from institution to institution. The Committee believes that the Federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission are equipped to establish *broad parameters* for such guidelines, but that *individual institutions are in the best position to determine how best to develop and implement the required policies and procedures*….

(Emphasis added)

The following statement in the Supplementary Information to the JNPR reflects this approach:

> … The agencies are not proposing to prescribe which Red Flags will be relevant to a particular type of financial institution or creditor. For this reason, the proposed Regulations provide that each financial institution and creditor must identify for itself which Red Flags are relevant to detecting the risk of identity theft….

71 Fed. Reg. at 40,791.

Notwithstanding this statement and the agencies' general recognition of the need to adopt a flexible, risk-based approach, certain language in the proposed rule and its likely enforcement scheme appear to supplant the regulated entities' relevancy determinations with their own. In addition to exceeding the statutory mandate, this may force entities to adopt measures that are designed more to protect against a regulatory enforcement action than actual threats of identity theft.

Our specific concern centers on the requirements that: (i) regulated entities develop and implement a written identity theft program that includes policies and procedures to identify Red Flags that are *relevant* to detecting a possible risk of identity theft; and (ii) regulated entities "have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft."[2]

The proposed rule does not define the term *relevant*, nor does it state that the relevancy determination rests with the regulated entity as opposed to the enforcing agency. The "reasonable basis" requirement can only be interpreted to require regulated entities to meet the enforcing agency's own standard of reasonableness and, of equal concern, it places the regulated entity in the awkward position of having to prove a negative. A more prudent approach (and one that is in harmony with congressional intent) would require regulated entities to demonstrate how the policies and procedures they have designed, pursuant to a risk evaluation that considers the delineated Red Flags, adequately address the threat of identity theft at their respective businesses. To require regulated entities to do more than demonstrate the effectiveness of their own programs will cause them to anticipate what the enforcing agency may require during an investigation and to tailor their identity theft programs accordingly. This misdirected approach will divert regulated entities' scarce resources from their intended object (the prevention of identity theft) and strip them of the entity-specific discretion that Congress intended.

Ability to Achieve Statutory Goals

In addition to our concerns about the proposed rule's consistency with the statutory mandate, we believe, in some cases, it will fail to fulfill the statute's goals. For example, it is conceivable that any number of the listed Red Flags may arise in an actual case of identity theft. An identity thief may have submitted a credit application with a phone number associated with an answering service (Red Flag 11b), a phone number that is shared with another customer of that institution (Red Flag 12), or incomplete information (Red Flag 13). However, such occurrences, particularly the receipt of incomplete credit applications, are not uncommon and almost always arise in transactions that do not involve identity theft. Identifying such attenuated occurrences as a trigger for additional compliance activity only serves to elevate an already high regulatory burden (see discussion below) without producing a corresponding benefit in identity theft prevention. To avoid this unintended result, the agencies should narrow the delineated Red Flags to those that indicate a reasonable likelihood of identity theft.

Ambiguous Nature of Requirements

It is unclear how certain requirements in the proposed rule apply to vehicle dealers and what specifically is expected of them. To remove this ambiguity, we request the agencies address the following queries:

---

[2] Proposed 16 C.F.R. § 681.2(d)(2)(iii). Because franchised automobile dealers fall within the scope provisions of proposed sections 681.1(a) and 682(a) of title 16 of the Code of Federal Regulations, these comments refer to citations contained in the FTC's portion of the JNPR.

1. Definitions

- Is a retail installment sales contract that is immediately assigned to a finance source an *account* as defined by proposed section 681.2(b)(1)? Although retail installment sales contracts are specifically identified in the definition of *account* and in the Supplementary Information, see 71 Fed. Reg. at 40,789, retail installment sales contracts that are assigned to a third-party finance source do not result in a "continuing relationship" between the initial creditor and the customer. Nor does a retail installment sales contract assigned to a bank appear to fit within the definition of an *account* as set forth in the federal banking agencies' joint final rules implementing section 326 of the USA PATRIOT Act. 68 Fed. Reg, 25,092-25,093 (May 9, 2003); see also FAQ 2 in the federal banking agencies' *Interagency Interpretive Guidance on Customer Identification Program Requirements under Section 326 of the USA PATRIOT Act* (Apr. 28, 2005). By its very nature, three-party vehicle financing transactions involve two creditors (the initial creditor and the assignee). To avoid imposing redundant requirements on separate entities for the same transaction, the definition of *account* should not extend to "relationships that are not 'continuing'…" 71 Fed. Reg. at 40,789.

- Does the *scope* provision in proposed section 681.2(a) extend to franchised medium- and heavy-duty truck dealers? These businesses rarely engage in transaction with consumers, although they may obtain credit reports during the vehicle financing application process in a limited number of transactions.

- The definition of *service provider* in the JNPR is very broad as it extends to any person that provides a service directly to the regulated entity. The agencies state that the "definition is based upon the definition of 'service provider' in the Agencies' standards implementing section 501(b) of the GLBA." 71 Fed. Reg. at 40,790. However, the Safeguards Rule definition limits the term to persons or entities that have access to customer information. 16 C.F.R. § 314.2(d). The definition of *service provider* in the JNPR contains no such qualifier even though the universe of service providers to whom the proposed rule applies is qualified indirectly in proposed section 681.2(d)(4)(by imposing the service provider requirement on persons that provide an activity on behalf of the regulated entity that are applicable to the requirements of its Identity Theft Prevention Program). For greater clarity, we suggest narrowing the definition of *service provider* to the persons described in that provision.

2. Identifying Relevant Red Flags

- Does the mere fact that a regulated entity requests customers to provide data that is mentioned in a delineated Red Flag require it to conclude that the Red Flag is relevant to detecting a possible risk of identity theft? Several of the delineated Red Flags identify items such as social security numbers (SSNs), addresses, and phone numbers that are routinely requested on applications for vehicle financing. Automobile and truck dealers do not typically perform such functions as matching the SSN that appears on an application to the Social Security Administration Death Master File (Red Flag 8b), determining whether a correlation exists between the SSN provided and the applicant's date of birth (Red Flag 9), comparing the address on an application to addresses on fraudulent applications (Red Flag 10a), checking addresses to ensure they are not fictitious (Red Flag 10b), and checking phone numbers to determine if they are invalid or associated with a pager or answering service (Red Flag 11b). (Of course, any irregularities noted during the sale, vehicle financing, insurance verification, registration, and titling process may generate additional steps to verify the identity of the purchaser.) Must vehicle dealers now regard these Red Flags as relevant? If so, must they develop processes for detecting them? Such a duty will require vehicle dealers to purchase information technology (IT) components necessary to perform these new functions, as manual checks are not feasible. Notwithstanding the agencies' attempt to "draft this section in a flexible, technologically neutral manner that would not require financial institutions or creditors to acquire expensive new technology to comply with the Red Flag Regulations," 71 Fed. Reg. at 40,791, it is difficult to imagine how regulated entities would perform this cross-checking function without incurring these expenses.

- Guidance is needed on what the agencies consider a reasonable basis for concluding that particular Red Flags do not evidence a risk of identity theft. For example, Red Flag 13 identifies a customer's failure "to provide all required information on an application." As noted above, it is a common occurrence at automobile and truck dealerships for customers not to complete all the required information on a credit application (in fact, this may occur in as many as half of the applications). The large number of customers who do not fill out all the required information significantly exceeds the very small number of customers who actually engage in identity theft. Does this fact alone mean that the Red Flag does not "evidence a risk of identity theft?" Proposed section 681.2(d)(2)(iii). Or does it trigger the need to "[a]ddress the risk of identity theft," proposed section 681.2(d)(2)(iv), in every transaction where this occurs?

3. <u>Detecting Relevant Red Flags</u>

- If a regulated entity determines that a Red Flag is relevant, can it rely on the detection process utilized by another entity that is involved in the same transaction? For example, in a three-party vehicle financing transaction, the dealer enters into a retail installment sales contract or a lease agreement with a customer that it immediately assigns to a third-party finance source (such as a bank or a credit company). In this situation, the assignee-finance source reviews the credit application and performs underwriting before the dealer and the customer enter into the agreement. If the assignee performs the cross-checking functions identified in several of the delineated red flags, must the initial creditor do the same? We assume not since such an exercise would be redundant and would only serve to increase the compliance burden imposed by the rule.

- In the preceding scenario, is the assignee considered a *service provider* of the initial creditor? We assume not, since the initial creditor does not retain the assignee to perform this function on its behalf. Instead, the assignee performs this function as part of its own underwriting process.

4. Addressing the Risk of Identity Theft

- Assuming a Red Flag is considered relevant and is detected, the proposed rule states that the regulated entity must address the risk of identity theft commensurate with the degree of risk posed and cites examples of actions that address the risk. Proposed section 681.2(d)(2)(iv). We request that the agencies provide several more examples of their expectations in the context of vehicle financing transactions.

5. Regulatory Guidance under Section 315

- Section 315 of the FACT Act directs the agencies to "prescribe regulations providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice of discrepancy…." These regulations must "describe reasonable policies and procedures for use by a user of a consumer report…." The agencies state in proposed section 681.1(c) that a user that "employs the policies and procedures regarding identification and verification set forth in the Customer Identification Program [CIP] rules implementing 31 U.S.C. 5318(l) under these circumstances satisfies this requirement, whether or not the user is subject to the CIP rules." Is utilization of the CIP policies and procedures the sole means of fulfilling this requirement, or will the agencies provide additional guidance to regulated entities not subject to the CIP requirements on other "reasonable policies and procedures" that a user may employ?

Burden Imposed on Vehicle Dealers

The proposed rule would impose an enormous burden on franchised automobile and truck dealers that is significantly understated in the FTC's burden estimate at 71 Fed. Reg. 40,800-40,801. Unlike banking entities, vehicle dealers are not subject to the CIP requirements under section 326 of the USA PATRIOT Act and thus cannot rely on previously established "know your customer" procedures to satisfy relevant portions of the Red Flags rule. Instead, it appears the agencies expect vehicle dealers to develop automated systems to detect several of the delineated Red Flags and create new procedures to assess and address the risk of identity theft presented by the identified Red Flags. These new duties are in addition to the new requirements to develop a written Identity Theft Prevention Program, conduct training, oversee service providers, and submit annual written reports to the regulated entities' boards of directors. These duties will require extensive employee time from each dealership and considerable costs in upgrades to existing IT systems. Because many dealerships lack the in-house expertise to oversee this process, they likely will turn to a cohort of vendors that will eagerly offer their technical compliance expertise and charge handsomely for it. This is precisely what happened when the FTC Safeguards Rule took effect, and it appears the complexity of the proposed Red Flags rule will easily surpass the compliance challenges presented by the Safeguards Rule.

If medium- and heavy-duty truck dealers fall within the FTC's scope provision at proposed section 681.2(a), the collective burden on vehicle dealers will be even greater. Unlike car and light-duty truck dealers, the nation's approximately 1,900 dealers who sell only medium- and/or heavy-duty trucks are not subject to the Safeguards Rule and thus cannot merely "combine [their] program[s] to prevent identity theft with [their] information security program." 71 Fed. Reg. at 40,788. Medium- and heavy-duty truck dealers will be starting from scratch, and it does not appear the FTC's burden estimate reflects this burden.

The FTC's burden estimate for vehicle dealers is flawed in other regards. It states, in part:

> FTC staff believes that motor vehicle dealers would incur less burden than other high-risk entities. Because their loans are typically financed by financial institutions that are also subject to these proposed regulations, FTC staff believes that motor vehicle dealers are likely to use the financial institutions' programs as a basis for developing their own programs. Accordingly, FTC staff estimates that to create and implement a written program that incorporates policies and procedures that high-risk entities already are likely to have in place, … it will take motor vehicle dealers 5 hours, with an annual recurring burden of 1 hour….

71 Fed. Reg. at 40,800.

In researching this statement, we have not received any indication that dealers will be able to "use financial institutions' programs as a basis for developing their own programs." Many assignee-financial institutions, like dealers, are not subject to the CIP requirements (e.g., automobile manufacturer finance subsidiaries) and thus will be similarly confronted with the need to adjust their existing anti-identity theft measures to the requirements of the Red Flags rule. Unless dealers in standard three-party vehicle financing contracts can routinely defer to the measures that assignee-financial institutions have adopted, dealers will not be able to simply incorporate the assignees' program elements into their own programs.

In addition, it is difficult to imagine how most regulated entities' compliance personnel would be able to read and fully understand the Red Flags rule requirements, let alone create *and implement* a written Identity Theft Prevention Program, in a 5-hour period. The Safeguards Rule experience of vehicle dealers is instructive. In 2003, dealers felt it necessary to review government and trade association literature, attend seminars, and frequently contact attorneys and accountants to determine how the general standards set forth in the Safeguards Rule applied to their industry and to their business operations. Even after becoming familiar with the Safeguards Rule, many sought the assistance of vendors to ensure their program was appropriately tailored to their particular business model. This demanded considerable time and expense and, as stated above, it appears the Red Flags rule will require an even greater compliance effort.

In addition, the implementation burden estimate should account for the new duties in Appendix J that currently are not part of a regulated entity's business model. To the extent vehicle dealers must execute on a per customer basis such duties as those identified in Red Flags 3, 8b, 9, 10a, 10b, and 11, the burden estimate should account for the additional time this will take (and the expenses it will generate if IT changes are necessary) in the over 16 million new vehicle transactions and over 25 million used vehicle transactions that are financed or leased on an annual basis.[3]

Regarding the FTC's training burden estimate (2 hours, with an annual recurring burden of 1 hour), we anticipate that the training required for vehicle dealership employee(s) who are responsible for implementing the program will easily exceed 2 hours. Employees at vehicle dealerships who must discharge this responsibility do so in conjunction with a host of unrelated business functions. They typically do not specialize in the development of compliance programs and therefore require more initial training than their counterparts at larger businesses.

In addition, depending on the agencies' interpretation of the duties imposed by several of these requirements, the training burden imposed on employees involved in vehicle financing may be far greater. For example, Red Flag 3 suggests a duty to use a certain methodology to review credit reports for an unusual pattern of activity. If vehicle dealers are expected to train their finance managers on this new methodology, their training burden will further increase.

Regarding the requirement in proposed section 681.2(d)(5)(iii)(A) that staff responsible for implementing the regulated entity's Identity Theft Prevention Program furnish a written compliance report to the board of directors, the agencies inquire into how frequently these reports should be furnished. At a minimum, the reports should be required no more than once per calendar year and the regulated entity should be given discretion to determine when during the calendar year the report must be filed (even if this results in more than 12 months elapsing between reports). By providing this flexibility, regulated entities can coordinate this reporting requirement with their other regulatory and administrative reporting requirements.

For the foregoing reasons, we request the agencies omit from the final rule burdens that exceed the statutory mandate and do not practically reduce the likelihood of identity theft. We also request the agencies address the queries presented in these comments to clarify vehicle dealers' compliance responsibilities. To the extent the agencies opt to provide such guidance in educational publications (see, e.g., FTC Facts for Business, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (republished April 2006); FTC Facts for Business, *The FTC's Privacy Rule and Auto Dealers: Frequently Asked Questions* (January 2005); FTC's *Frequently Asked Questions for the Privacy Regulation* (December 2001)), we request the agencies issue the guidance sufficiently *before* the final rule takes effect to ensure regulated entities can benefit from it while developing their Identity Theft Prevention Programs. Further, we encourage the agencies to provide in the final rule and their educational publications as much illustrative guidance as possible on measures that comply with the section 114 and section 315 requirements.

Finally, in order to provide small businesses that do not have formal CIP procedures in place the opportunity to develop an effective and compliant Identity Theft Prevention Program, we request

---

[3] CNW Marketing Research, Inc. (2004 data). The figure for used vehicle transactions that are financed or leased includes private transactions not involving franchised or independent dealers.

the agencies establish a compliance date that is at least 18 months after the date in which the final rule is published in the *Federal Register*. Our requests for a reduced regulatory burden, additional guidance, and an 18-month compliance period comport with House Financial Services Committee Chairman Oxley's expectation that the agencies will "take into account the limited personnel resources available to smaller institutions and craft such regulations and guidelines in a manner that does not unduly burden these smaller institutions." JNPR, Footnote 19.

Conclusion

We appreciate the opportunity to submit these comments and the agencies' consideration of our concerns. Please contact us if we can provide additional information that would be useful in the development of the final rule.

We will coordinate with the FTC's professional staff shortly after the final rule is issued to ensure we can disseminate necessary compliance information well in advance of the rule's effective date.

Sincerely,

Paul D. Metrey
Director, Regulatory Affairs