Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003
The Red Flags Rule, Project No. R611019

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

I. BACKGROUND

The President signed the Fair and Accurate Credit Transactions Act (the FACT Act), which amended the Fair Credit Reporting Act of 1970 (FCRA), into law on December 4, 2003. Pub. L. 108–159 (2003). The FACT Act was implemented in part to assist in the detection, prevention, and mitigation of identity theft. Section 114 of the FACT Act amends Section 615 of the FCRA and requires the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission (the Agencies) to issue guidelines on identity theft for financial institutions and creditors (covered entities). These guidelines are meant to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

The Agencies are also proposing joint regulations requiring covered entities to establish reasonable policies and procedures for implementing the guidelines. More specifically, the Agencies are proposing to implement the requirements of Section 114 through Red Flag Regulations that would require financial institutions and creditors to implement a written Identity Theft Prevention Program (Program). The Program must contain reasonable policies and procedures to address the risk of identity theft. The Agencies also are proposing Red Flag Guidelines that require financial institutions and creditors to incorporate relevant indicators of identity theft into their Programs.

Section 315 of the FACT Act amends Section 605 of the FCRA and requires consumer reporting agencies to provide a notice of the existence of a discrepancy if the address provided by the user of a consumer report "substantially differs" from the address the consumer reporting agency has on file. The Agencies are proposing joint regulations that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when it receives a notice of address discrepancy from a consumer reporting agency.

On July 18, 2006, the Agencies issued a joint notice of proposed rulemaking and requested comments to be submitted by September 18, 2006 on the proposed Red Flag Regulations and Guidelines and the Proposed Regulations Implementing Section 315. The National Independent Automobile Dealers Association (NIADA) has represented independent motor vehicle dealers for 60 years. The National Association and its State Affiliate Associations represent more than 20,000 motor vehicle dealers located across the United States. In 2005, over 30.6 million used motor vehicles were retailed by motor vehicle dealers generating more than $311 billion in revenues. Because vehicles are lasting longer (the average vehicle on the road today is over 7.8 years old), projections of future used vehicle sales volumes suggest that the retail used motor vehicle market will maintain its 30-million-plus volume in the years to come.[1] Given the

[1] The 2006 Used Car Market Report, Manheim Auctions, 1400 Lake Hearn Drive, NE, Atlanta, GA 30319 1464.

number of motor vehicle transactions that take place each year, the Red Flag Regulations and Guidelines will have a significant impact on the used retail motor vehicle industry.

II. COMMENTS PERTAINING TO SECTION 114 OF THE FACT ACT

A. Overview

The Agencies are proposing Red Flag Regulations that adopt a flexible risk-based approach similar to the approach used in ‘Standards for Safeguarding Customer Information’’ issued by the FTC, to implement Section 501(b) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801. Under the proposed Red Flag Regulations, financial institutions and creditors must have a written Program that is based upon the risk assessment of the financial institution or creditor and that includes controls to address the identity theft risks identified. The Agencies note that like the program described in the Agencies' Information Security Standards, the Red Flag Program must be appropriate to the size and complexity of the covered entity and the nature and scope of its activities, and be flexible enough to address changing identity theft risks as they arise. In addition, financial institutions and creditors may combine the Program to Prevent Identity Theft with the Information Security Program. To ensure the Program's effectiveness, each covered entity must monitor, evaluate and adjust its Program, including the type of accounts covered. The following comments focus on sections of the Proposed Regulations and Guidelines that NIADA feels will have the most direct impact on its Members.

B. Proposed Red Flag Regulations: Section-by-Section Analysis of Proposed Definitions

1. Proposed Definition of “Account”

The proposed definition of ‘‘account’’ is similar to the definition of ‘‘customer relationship’’ found in the Agencies' Privacy Regulations. ‘‘Account’’ is defined as ‘‘a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12U.S.C. 1843(k).’’ The definition gives examples of an ‘‘account’’ including an extension of credit for personal, family, household or business purposes, such as a retail installment sales contract, including a car loan or lease. The Agencies further state that the risk-based nature of the proposed Red Flag Regulations affords each financial institution or creditor flexibility to determine which relationships will be covered by the Program through a risk evaluation process. The Agencies requested comments regarding the scope of the proposed definition of “account,” whether the definition should include relationships that are not “continuing,” and whether additional or different examples of accounts should be added to the Regulations.

NIADA supports limiting the definition of accounts to include only those relationships that are continuing. The definition of “account” and the scope of the definition should closely parallel the definition of “customer relationship” in the Agencies' Final Privacy and Safeguards Rules. NIADA further avers that the Agencies should clarify the difference between a “new account” and “existing account” and when a “continuing relationship” is deemed to be established for the various purposes of the Proposed Regulations. For example, while the vast majority of motor vehicle dealers will be subject to those provisions in the Regulations that impose an obligation upon covered entities to verify the identity of customers opening new accounts, fewer motor vehicle dealers will maintain a “continuing relationship” with the individual that opens a new account.

When the FTC adopted its Final Privacy Rules, it 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 or creditor, the customer records and information are also transferred to that institution. 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 comply with those provisions of the Regulations that apply only to "existing accounts" or that apply only when a continuing relationship with the consumer exists. The entity receiving the information should be required to comply with these provisions in the Red Flag Regulations.

Having consistency with terms used in the Agencies' Final Privacy and Safeguards Rules, should minimize the disruption of the existing practices of entities that have implemented policies and procedures to comply with other measures adopted to protect consumer information in accordance with applicable Federal and State Laws.

2. Proposed Definition of "Customer"

The Agencies solicited comment regarding the scope of the proposed definition of "customer," which would encompass both ''customers'' and ''account holders,'' i.e. any a person that has an account with a financial institution or creditor. As the Agencies point out, this proposed definition is broader than the definition of customer in the Information Security Standards because it applies to any ''person,'' including any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity. The Agencies further clarify that a financial institution or creditor would have the discretion to determine which type of customer accounts will be covered under its Program, since the Proposed Red Flag Regulations are risk-based.

NIADA believes that the definition of "customer" and the scope of the definition should closely parallel the definition of customer in the Agencies' Final Privacy and Safeguards Rules, neither of which apply to information obtained from other business entities. However, NIADA is not strongly opposed to the inclusion of governmental and business entities in the Red Flag Regulation's definition of "customer." As stated by the Agencies, these types of entities can likewise be victims of identity theft and financial institutions and creditors will have discretion to determine whether these types of accounts should be covered under their individual Programs. Moreover, these Regulations are not the first to be adopted that would apply to a broader scope of customers. For example, the FTC's Disposal Rule, which was also promulgated pursuant to the FACT Act, applies to information obtained about any individual, even in a business-to-business transaction. NIADA does not believe that including this broader definition will impose significant new burdens on NIADA Members, many of whom have already adopted and implemented policies and procedures to comply with the FTC's Privacy, Safeguards and Disposal Rules and apply these policies to information collected from any customer, consumers and business entities alike.

3. Proposed Definition of a "Service Provider"

The Agencies propose to define a "service provider" as "a person that provides a service directly to the financial institution or creditor." NIADA submits that this definition is overly broad and

should be modified to clarify that a "service provider" is deemed to be "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer or account information through its provision of services directly to a financial institution or creditor that is subject to the rule." This definition would be consistent with the definition in the Information Security Standards and the provisions in the Agencies' Proposed Red Flag Regulations governing "oversight of service provider arrangements." The definitions utilized in the Red Flag Regulations and Information Security Standards, whenever possible, should be consistent and bear the same meaning so as to avoid confusion. The Agencies should also refrain from establishing rules that apply to persons or entities not otherwise subject to their respective jurisdictions.

C. Development and Implementation of the Identity Theft Prevention Program

1. Identification and Evaluation of Red Flags

Proposed paragraph § _____.90(c) describes the primary objectives of the Identity Theft Prevention Program. Each financial institution or creditor must implement a written Program in the manner described in § _____.90(d). Under proposed paragraph §____.90(d)(1)(i), the Program must include policies and procedures to identify which Red Flags are relevant to detecting the possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor using the risk evaluation described in §____.90(d)(1)(ii). At a minimum, the Program must incorporate any relevant Red Flags from proposed Appendix J (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation), applicable supervisory guidance, incidents of identity theft that the entity has experienced and methods of identity theft that the entity has identified that reflect changes in identity theft risks.

Recognizing that the Red Flag Regulations will apply to a wide variety of different financial institutions and creditors, the Agencies are not proposing to prescribe which Red Flags will be relevant to a particular entity, but rather leave it to the entity to identify for itself on a continuing basis which Red Flags are relevant taking into consideration the types of accounts and customers that are subject to a risk of identity theft, the methods it provides to access these accounts, its size, complexity, and location, and the nature and scope of its activities. As the Agencies point out, each financial institution or creditor must monitor, evaluate, and adjust its Program on a continuing basis to identify any additional Red Flags that are relevant to detecting a possible risk of identity theft.

NIADA appreciates the FTC's decision to include guidelines to assist entities to assess the risk of identity theft to customers or to the safety and soundness of the entity using the risk evaluation and is in agreement with the decision to allow covered entities to decide for themselves which Red Flags are relevant to their organization. NIADA believes that the enumerated sources of Red Flags are appropriate, but urges the Agencies to include examples of the Red Flags that may be relevant to detecting the risk of identity theft based upon the types of accounts and activities engaged in by the covered entities. It would be beneficial for those attempting to understand and comply with the Red Flag Regulations, especially small businesses, to have illustrative examples of the types of Red Flags that are "relevant" in a given situation.

The flexibility of the Proposed Regulations, together with examples providing guidance on the types of Red Flags that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor should help to protect both the covered entities and their customers. In addition, the ability of financial institutions and

creditors to combine their Red Flags Program with their Information Security Program and procedures implemented to comply with the CIP Rules should minimize the disruption of the existing practices of entities that have implemented policies and procedures to protect consumer information and prevent fraud. This will also help minimize the burdens and costs of complying with the Red Flag Regulations, while increasing the likelihood that customer information is adequately protected.

2. Identity Theft Prevention and Mitigation

Proposed § _____.90(d)(2) states that the Program must include reasonable policies and procedures designed to prevent and mitigate identity theft in connection with the opening of an account or any existing account. Some of the policies and procedures relate solely to account openings, while others relate to existing accounts. Pursuant to subsections (i)-(iv), the Program must include reasonable policies and procedures to: (i) obtain identifying information about and verify the identity of, a person opening an account; (ii) detect the Red Flags identified pursuant to paragraph § _____.90(d)(1); (iii) assess whether the Red Flags the financial institution or creditor has detected evidence a risk of identity theft (and, if it determines that a Red Flag does not evidence a risk of identity theft, have a reasonable basis for so concluding); and (iv) take appropriate measures to address the risk of identity theft to the customer, the financial institution, or creditor, commensurate with the degree of risk posed.

The Agencies noted that with respect to the provision requiring entities to obtain identifying information about and verify the identity of a person opening an account, some financial institutions and creditors are already subject to the CIP Rules, which require verification of the identity of customers opening accounts. Therefore, the Agencies have specified that any financial institutions and creditors may satisfy the Red Flag requirements by applying the policies and procedures for identity verification that they have developed to comply with the CIP Rules. The only caveat is that the Red Flag Regulations cover a variety of entities and products and relationships that are excluded from the CIP Rules.

With respect to the requirement that the Program must include policies and procedures that address the risk of identity theft to the customer, the financial institution, or creditor, commensurate with the degree of risk posed, the Regulations provide an illustrative list of measures that a financial institution or creditor may take, including, but not limited to, monitoring an account for evidence of identity theft; contacting the customer; not opening a new account or closing an existing one, and notifying law enforcement. Some of the measures identified are actions that have to be taken by entities subject to the CIP Rules, Section 112 of the FACT Act and Section 623 of the FCRA. The Agencies solicited comments on whether the enumerated measures should be included as examples that a financial institution or creditor may take and whether additional measures should be included.

NIADA agrees with the Agencies that it is appropriate for those entities that already comply with the CIP Rules to be deemed to be in compliance with the identity verification requirements under the Red Flag Regulations since the factors that must be considered are almost identical. It is much less burdensome for covered entities to apply their existing policies and procedures to other accounts that are not covered by the CIP Rules than to adopt a whole new set of policies and procedures to comply with the identity verification requirements under the Red Flag Regulations.

NIADA is opposed, however, to the obligations imposed on financial institutions and creditors to assess whether a Red Flag evidences a risk of identity theft and their burden to prove they had

a reasonable basis for concluding that a Red Flag did not evidence a risk of identity theft; not to mention a covered entity's potential liability if, not notwithstanding having established the required policies and procedures, an incident of identity theft occurs. The Agencies themselves recognize that some Red Flags that are relevant today may become obsolete and that it may be difficult even for the Agencies to update Appendix J quickly enough to keep pace with rapidly evolving patterns of identity theft.[2]

Moreover, some of the examples of Red Flags are unduly burdensome and may not even be feasible for many of the covered entities to monitor. For instance, motor vehicle dealerships do not have access to information to determine if a "social security number has not been issued or is listed on the Social Security Administration's death master file." Nor are they equipped to evaluate whether a customer's credit report reflects a recent and significant increase in the volume of inquiries, a material change in the use of credit, or a material change in purchasing or spending patterns, not to mention whether such variations are reasonably explainable. In a large majority of motor vehicle transactions, the dealership is merely assisting its customer to obtain financing by helping the customer complete a credit application and pulling a credit report to provide to a third party lending source. Often times they are not evaluating the credit information provided or making a decision as to whether or not credit should be extended. In those situations where a dealership is the entity making a credit decision or servicing an account, it has to weigh the potential liability if it errs in declining to open an account, closes an account or takes other actions to limit the availability of credit.

At a minimum, the Agencies should include examples of factors that may indicate that a Red Flag does not evidence a risk of identity theft, examples of how to mitigate incidents of identity theft, and a list of measures that a financial institution or creditor may take if there appears to be evidence of a risk of identity theft. NIADA believes that it is beneficial for those attempting to understand and comply with the Red Flag Regulations to have illustrative examples of the factors that should be considered and the appropriate measures that may be taken. The Agencies should also include a safe harbor provision in the Regulations for those entities that do establish and maintain a Program that is designed to effectively detect, prevent and mitigate identity theft in accordance with the Regulations and Guidelines if an incident occurs notwithstanding the implementation and maintenance of such polices and procedures.

3. Oversee Service Provider Arrangements

Proposed paragraph §_____.90(d)(4) states that whenever a financial institution or creditor engages a service provider to perform an activity on its behalf that is covered by the Red Flag Regulations, the entity must take steps to ensure that the activity is conducted in compliance with a Program that meets the requirements of the Regulations. This provision would, however, allow a service provider that provides services to multiple financial institutions and creditors to conduct activities on behalf of these entities in accordance with its own Program to prevent identity theft, as long as the Program complies with the Regulations.

The Agencies requested comments on whether permitting a service provider to implement a Program that differs from the Program of a financial institution or creditor to whom it is providing services would fulfill the objectives of the Red Flag Regulations. The Agencies also requested comments on whether it is necessary to address service provider arrangements in the Red Flag Regulations, or whether it is self-evident that a financial institution or creditor remains

[2] See Federal Register, Vol. 71, No. 137 at 40791.

responsible for complying with the standards set forth in the Regulations, even when it contracts with a third party to perform an activity on its behalf.

The NIADA agrees with the approach taken by the Regulations with regard to allowing a service provider to implement its own Program to comply with the requirements. As to whether it is necessary to address the service provider arrangements in the Regulations, NIADA prefers the approach taken by the Agencies under the CIP Rules, which do not contain a service provider provision. Whether the parties elect to mandate compliance with the Regulations as part of their contractual agreement should be at the entities' own discretion and should be part of their risk assessment and the implementation of the Program it deems appropriate to protect both itself and its customers. For example, a financial institution may take into consideration whether a service provider is subject to the Information Security Standards or other federal or state laws that impose a duty to protect customer and account information consistent with the Red Flag Regulations, and the degree of sensitivity of the information to which the third party provider has access.

Whether the Agencies elect to take the approach under the CIP Rules or the approach taken under the Information Security Standards (where financial institutions must require their service providers by contract to safeguard customer information in a manner that meets the objectives of the Standards), NIADA is opposed to any requirement that would impose an obligation upon the financial institution to continuously oversee or monitor a service provider's compliance with the Regulations. NIADA asserts that such an obligation would be impossible to satisfy and if a financial institution provides information and records to another entity, that entity is responsible for knowing its obligations under applicable Federal and State Laws. Motor vehicle dealerships may have numerous locations and service providers and it would be nearly impossible to monitor whether every lender, financial institution, and third party service provider is complying with the Regulations.

4. Involve the Board of Directors and Senior Management

Proposed §____.90(d)(5) sets forth the responsibility of the board of directors and senior management to develop and implement a Program that complies with the Red Flag Regulations. In the case of any creditor that does not have a board of directors, "board of directors" is defined as a designated employee. The board of directors or an appropriate committee of the board must approve the written Program.

The board, an appropriate committee of the board, or senior management is also charged with overseeing the development, implementation, and maintenance of the Program, including assigning specific responsibility for its implementation. In addition, persons charged with overseeing the Program must review reports prepared at least annually by staff regarding compliance by the financial institution or creditor with the Red Flag Regulations. The reports must discuss material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for changes in the Program. The Agencies requested comments on the frequency with which reports should be prepared and whether responsibility for oversight and implementation of the Program is properly allocated between the board and senior management.

NIADA believes that requiring the preparation of written reports that have to be and approved on

an annual basis is overly burdensome, especially for small businesses. In the case of smaller financial institutions and creditors, there are fewer employees available to provide instruction on compliance, let alone to prepare lengthy written reports. The average independent motor vehicle dealership, for instance, has 5 or fewer employees.[3] Similar to the Information Security Standards, it would be sufficient if the Agencies mandated that covered entities continuously review and evaluate the policies and procedures adopted and modify them as necessary to achieve the purposes of the FACT Act and Implementing Rules. When and how often a financial institution or creditor assesses the potential threats should be left to the discretion of the covered entity and would be relevant as to whether it has developed "reasonable" policies and procedures. Likewise, the appointment of an individual or committee to be responsible for overseeing the development, implementation, and maintenance of the Programs should be at the discretion of the financial institution or creditor taking into account the size and complexity of the entity.

D. Proposed Red Flag Guidelines: Appendix J

Section 114 of the FACT Act provides that the Agencies, in developing the guidelines, must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The Agencies have identified Red Flags relevant to detecting a possible risk of identity theft in Appendix J. Recognizing that a wide range of financial institutions and creditors, as well as a broad variety of accounts, will be covered by the Regulations, the Agencies have clarified that the list is not meant to be exhaustive. They have provided each financial institution and creditor with the flexibility to develop policies and procedures to identify which Red Flags in the Appendix are relevant to detecting the possible risk of identity theft. The Agencies solicited comments on whether the proposed Red Flags listed in Appendix J are too specific or not specific enough and whether additional or different Red Flags should be included.

Because proposed §___.90(d)(1) of the Red Flag Regulations provides that each financial institution and creditor must have policies and procedures to identify "additional Red Flags from applicable supervisory guidance that may be issued from time to time, incidents of identity theft that the financial institution or creditor has experienced, and methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks,"[4] NIADA agrees that the Red Flags listed in Appendix J are specific enough and that it is not necessary at this time to include additional Red Flags. NIADA commends the Agencies on recognizing that each entity covered by the Red Flag Regulations may face different identity threats and that these threats change over time. Allowing and encouraging covered entities to develop Red Flags that suit their specific business practices will help to ensure that the goals of the Regulations are met.

III. SECTION 315 OF THE FACT ACT

A. Overview

Section 315 of the FACT Act amends Section 605 of the Fair Credit Reporting Act by adding a new section (h) which requires that, when providing consumer reports to requesting users,

[3] 2006 NIADA Independent Used Car Industry Report, National Independent Automobile Dealers Association, 2521 Brown Blvd., Arlington, TX 76006, and Leedom, and Associates, LLC, 40 Sarasota Center Blvd., Suite E, Sarasota, FL 34277.

[4] Fed. Reg. Vol. 71, No. 137 at 40794.

consumer reporting agencies must provide a notice of the existence of a discrepancy if the address provided by the user in its request ''substantially differs'' from the address the Credit Reporting Agency has in the consumer's file. The scope of Section 315 is different than that of Section 114 in that it applies to "users of consumer reports" and "persons requesting consumer reports."

The Agencies are required to issue regulations that provide guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy. These regulations must describe reasonable policies and procedures for users of consumer reports to "(i) enable them to form a reasonable belief that the user knows the identity of the person for whom it has obtained a consumer report, and (ii) reconcile the address of the consumer with the Credit Reporting Agency, if the user establishes a continuing relationship with the consumer and regularly and in the ordinary course of business furnishes information to the Credit Reporting Agency."[5]

B. Proposed Regulation Implementing Section 315: Section-by-Section Analysis

1. Requirement to Form a Reasonable Belief

Proposed § _____.82(c) states that a user of a consumer report must develop and implement reasonable policies and procedures for ''verifying the identity of the consumer for whom it has obtained a consumer report'' whenever it receives a notice of address discrepancy. These policies and procedures must be designed to enable the user to form a reasonable belief that it knows the identity of the consumer for whom it has obtained a consumer report, or determine that it cannot do so. This section also provides that if a user employs the policies and procedures regarding identification and verification set forth in the CIP Rules under the USA PATRIOT ACT, it satisfies the requirement to have policies and procedures to verify the identity of the consumer.[32] The Agencies requested comments on whether the CIP procedures are sufficient to allow a user of a consumer report to form a reasonable belief that it knows the identity of the consumer.

NIADA supports the Agencies' proposal to allow compliance with the CIP Rules to satisfy the requirements in Section 315 of the FACT Act as they pertain to verifying the identity of consumers during the opening of new accounts. The information collected from a consumer pursuant to the CIP Rules are appropriate and sufficient to enable a user of a consumer report to verify the identity of a customer for whom an address discrepancy is received at that time. They require that, at a minimum, the consumer's name, date of birth, address, and government-issued identification (such as a drivers license or passport) or verification through non-documentary methods such as contacting a customer or independently verifying the consumer's identity through the comparison of information provided by another source (i.e. checking references), be collected when an account is opened.[6]

Most motor vehicle dealers and other users of credit reports will already have procedures in place to comply with the CIP Rules, at least with respect to the opening of new accounts, and other entities may adopt the CIP Rules and apply them as appropriate. For those entities that are already required to comply with the CIP rules, compliance with Section 315 will be less burdensome. This requirement will also benefit both consumers and users by reducing the

[5] Fed. Reg. Vol. 71, No. 137 at 40795.
[6] 31 CFR 103.121.

likelihood that the wrong consumer report is used in making a decision about a consumer's eligibility for a product and assisting the user to detect whether a consumer about whom it has requested a consumer report is engaged in or a victim of identity theft.

2. Requirement to Furnish Consumer's Address to a Consumer Reporting Agency

Proposed § ____.82(d)(1) provides that a user must develop and implement reasonable policies and procedures for furnishing to the credit reporting agency from whom it receives a notice of address discrepancy an address for the consumer that the user has reasonably confirmed is accurate when the following three conditions are satisfied: (i) the user is able to form a reasonable belief that it knows the identity of the consumer for whom the consumer report was obtained; (ii) the user furnishes the address to the credit reporting agency if it establishes or maintains a continuing relationship with the consumer; and (iii) if the user regularly and in the ordinary course of business furnishes information to the credit reporting agency from which a notice of address discrepancy pertaining to the consumer was obtained. The consumer's address must be communicated to the credit reporting agency as part of the information the user regularly provides.

Section 315 also requires the Agencies to prescribe regulations describing reasonable policies and procedures for a user ''to reconcile the address of the consumer'' about whom it has obtained a notice of address discrepancy with the credit reporting agency ''by furnishing *such* address'' to the credit reporting agency. The Agencies are proposing to interpret the phrase, ''such address,'' as an address that the user has reasonably confirmed is accurate and, therefore, would require a user to take steps to ''reconcile'' the address it initially received from the consumer when it receives a notice of address discrepancy rather than simply furnishing the initial address it received to the credit reporting agency.

Proposed § _____.82(d)(2) contains a list of illustrative measures that a user may employ to reasonably confirm the accuracy of the consumer's address, such as: verifying the address with the person to whom the consumer report pertains; reviewing its own records of the address provided to request the consumer report; verifying the address through third-party sources; or using other reasonable means. The Agencies solicited comments on whether the regulations should include examples of measures that may be used to reasonably confirm the accuracy of the consumer's address, and whether different or additional examples should be listed.

The Agencies noted that these statutory requirements only apply if the user establishes a "continuing relationship" with the consumer. A user may also receive a notice of address discrepancy in connection with a consumer with whom it already has an existing relationship as well. NIADA interprets the statutory and regulatory provisions as meaning that in a situation where a motor vehicle dealership or other financial institution transfers or assigns an account to another financial institution or lender, the recipient financial institution is the entity that "establishes or maintains a continuing relationship" or "existing relationship" with a consumer and is responsible for responding to address discrepancy inquiries that arise pursuant to these provisions.

A motor vehicle dealership may obtain customer information, including a credit application, a credit report, and other documents related to the purchaser's credit history and ability to pay, in order to assist a consumer to obtain credit from a lender. NIADA acknowledges that under the CIP Rules and the Red Flag Regulations, as well as most of the dealerships contractual agreements with the financial institutions and lenders that actually extend the financing, it has

an obligation to verify the identity of the consumer at the time of taking the application information. However, the financial institution to which the application and credit report are submitted typically evaluates and verifies the information provided and makes the decision as to whether or not to extend credit and the terms upon credit will be extended. In addition, upon completion of the sales or lease transaction, the original records are transferred to the financial institution that agrees to extend the credit or service the loan. NIADA submits that the recipient financial institution will establish and maintain the continuing relationship with the consumer and will be in a better position to provide address discrepancy information to the credit reporting agency regarding an existing account and to assist with reconciling such discrepancies. NIADA requests that the Agencies clarify that this is the correct interpretation.

3. Timing

The Agencies requested comments on whether the timing for responding to notices of an address discrepancy is appropriate. Section 315 states that a user must provide a consumer's address to a Credit Reporting Agency for the reporting period in which the user's relationship with the consumer is established. Under proposed §____.82(d)(3)(i), which applies to new relationships, a user must therefore furnish the consumer's address that it has reasonably confirmed to the Credit Reporting Agency as part of the information it regularly furnishes for the reporting period in which it establishes the relationship with the consumer. If a user receives a notice of address discrepancy in other circumstances (i.e. with respect to an existing account), Proposed §_____.82(d)(3)(ii) states that the user should furnish this information for the reporting period in which it has reasonably confirmed the accuracy of the address.

As the Agencies point out, these timing requirements for the newly established relationships differ from those in the CIP Rules. The CIP Rules permit an account to be opened if certain identifying information is provided and users must verify the account within "a reasonable time period" after it has been opened. Because the Proposed Regulations state throughout that having policies and procedures in place that comply with the CIP Rules satisfies the requirement to have policies and procedures to verify the identity of a consumer, the time period for verifying the address of a consumer should be the same as that provided for in the CIP Rules. This will avoid even more unduly confusing, costly and burdensome requirements from being imposed on entities covered under the new Regulations.

C. Estimated Hours Burdens

NIADA appreciates the difficulty of the task imposed upon the FTC in establishing and implementing Red Flag Regulations and Guidelines for the wide range of financial institutions and creditors subject to its jurisdiction. With respect to the motor vehicle industry and Section 114 of the FACT Act, the FTC has estimated that it will take motor vehicle dealers 5 hours to create and implement a written Program that incorporates the polices and procedures, with an annual recurring burden of 1 hour. The FTC Staff also estimated that the incremental time to train staff to implement the Program will take high-risk entities (including motor vehicle dealers) 2 hours, with an annual recurring burden of 1 hour, and that preparation of an annual report would take these entities 4 hours (with an annual recurring burden of 1 hour).

With respect to Section 315, the FTC Staff estimated that it may take a small user no more than 16 minutes to develop and comply with the policies and procedures that it will employ when it receives a notice of address discrepancy, whereas a large user may take 1 hour. Similarly, the FTC Staff estimated that, during the remaining two years of the clearance, it may take a small user no more than 1 minute to comply with the policies and procedures that it will employ when

it receives a notice of address discrepancy, whereas a large user may take 45 minutes.

The Proposed Regulations implementing Section 315 also require a user of consumer reports to furnish an address that the user has reasonably confirmed is accurate to the consumer reporting agency from which it receives a notice of address discrepancy, but only to the extent that such user regularly and in the ordinary course of business furnishes information to the consumer reporting agency. The FTC Staff indicated that it believes that only 10,000 of the 1,658,758 users of consumer reports furnish information to consumer reporting agencies as part of their usual and customary business practices and that it will take such users 30 minutes to develop the policies and procedures for furnishing the correct address and that they will have automated the process of furnishing the correct address in the first year resulting in no annual recurring burden.

NIADA respectfully submits that the FTC's assessment of the estimated burdens for motor vehicle dealers to implement Section 114 of the FACT Act and the Implementing Regulations is vastly underestimated. Likewise, NIADA believes that the FTC has underestimated both the number of financial institutions that will be subject to the provisions in Section 315 of the Act and the estimated burdens.

For example, the FTC Staff noted in its estimated burdens analysis concerning Section 114 that "motor vehicle dealers would incur less burden than other high risk entities".[7] The rationale provided is that their loans are typically financed by financial institutions that are also subject to these Proposed Regulations and, therefore, the FTC Staff believes that motor vehicle dealers are likely to use the financial institutions' programs as a basis for developing their own programs. NIADA strongly disagrees.

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 types of financial services and products they provide, the amount of records they generate, how they retain records, and the systems to which they have access. In addition, the records and information a motor vehicle dealership obtains from a customer depends upon the structure of the transaction (sale or lease), as well as the types of financing involved (traditional or subprime, third party or in-house).

Moreover, it is incorrect to assume that any motor vehicle dealer will simply adopt an identity theft prevention program established by another financial institution. Some dealerships have relationships with dozens of financial institutions and creditors, while others have few, if any. There are a significant number of motor vehicle dealers that finance motor vehicle sales transactions themselves. In a recent survey of NIADA Members, 40.3% of the responding motor vehicle dealers indicated that they offer in-house or "buy here-pay here" financing (The Dealership itself finances the consumer's motor vehicle purchase).[8] Industry estimates place the total sales volume of buy here-pay here transactions between $80 and $110 billion per year,

[7] Fed. Reg. Vol. 71, No. 137 at 40800.

[8] 2006 NIADA Independent Used Car Industry Report, National Independent Automobile Dealers Association, 2521 Brown Blvd., Arlington, TX 76006, and Leedom, and Associates, LLC, 40 Sarasota Center Blvd., Suite E, Sarasota, FL 34277.

representing almost 8.5 to 10 million motor vehicle sales.[9] Approximately 24 million consumers are driving buy here-pay here financed vehicles today.[10] Additionally, many motor vehicle dealers own and operate separate related finance companies to which the dealership's finance contracts are sold and assigned. These entities would be subject to the requirements under both Sections 114 and 315.

To date, motor vehicle dealerships have adopted their own polices and procedures and programs to comply with laws and regulations pertaining to the protection of customer information and the prevention of fraud and identity theft, including, but not limited to: the Gramm-Leach-Bliley Act and the Privacy and Information Security Standards promulgated thereunder; the FACT Act and its Implementing Regulations, such as the Disposal Rules; and the CIP Rules that implement the USA PATRIOT Act. NIADA asserts that they will have to establish their own policies and procedures to comply with the Red Flag Regulations and Guidelines as well.

NIADA commends the Agencies for providing general standards and flexibility to covered entities to implement the Red Flag Regulations while taking into consideration each financial institution's size, the nature and scope of its activities, the standard practices in the industry and the specific experiences of that entity. The flexibility of the Proposed Regulations, together with examples providing guidance on the types of Red Flags that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution or creditor should help to protect both the covered entities and their customers.

In addition, the ability of financial institutions and creditors to combine their Red Flag Program with their Information Security Program and procedures implemented to comply with the CIP Rules should minimize the disruption of the existing practices of entities that have implemented policies and procedures to protect consumer information and prevent fraud. This will also help minimize the burdens and costs of complying with the Red Flag Regulations, while increasing the likelihood that customer information is adequately protected.

Notwithstanding the foregoing, NIADA believes that most, if not all, motor vehicle dealerships and other financial institutions will have to retain the services of consultants to advise them of their responsibilities under the FACT Act and the Agencies' Red Flag Regulations and Guidelines. The actual costs and burdens associated with developing a comprehensive Identity Theft Prevention Program in written form will vary from institution to institution depending upon a number variables, including: The type of business conducted; the size of the institution; the number of service providers with which it shares information; the number of employees; and the polices 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 significant**.**

NIADA believes there are ways that the costs and burdens of complying with the Regulations and Guidelines may be reduced and the benefits afforded to customers enhanced further. For instance, any definitions and requirements under the Regulations should be consistent with other similar regulations, like the Information Security Prevention and CIP Rules. The Agencies should also include additional guidelines to assist financial institutions to develop, implement

[9] Analysis of the Buy Here-Pay Here Capitalization Market, December 2003, Leedom and Associates, LLC, 40 Sarasota Center Blvd., Suite E, Sarasota, FL 34277.
[10] Industry Overview Keynote Remarks, Chris Leedom, October 2003 National Special Finance/Buy Here-Pay Here Conference.

and maintain an Identity Theft Prevention Program, as well as specific examples of mechanisms and/or polices and procedures that the FTC would consider relevant and reasonable to identify and mitigate risks of identity theft.

NIADA further submits that the Agencies failed to adequately take into account the limited personnel and resources available to smaller institutions and to craft the Proposed Regulations and guidelines in a manner that does not unduly burden them. In the case of smaller financial institutions and creditors, there are fewer employees available to provide instruction on compliance with new regulatory obligations and requiring written reports and approval on an annual basis is overly burdensome. For instance, the average independent dealership has 5 or fewer employees.[11]

Similar to the Information Security Standards, it would be sufficient if the Agencies mandated that covered entities continuously review and evaluate the policies and procedures adopted and modify them as necessary to achieve the purposes of the FACT Act and Implementing Rules. When and how often a financial institution or creditor assesses the potential threats should be left to the discretion of the covered entity and would be relevant as to whether it has developed "reasonable" polices and procedures. Likewise, the appointment of an individual or committee to be responsible for overseeing the development, implementation, and maintenance of the Programs should be at the discretion of the financial institution or creditor taking into account the size and complexity of the entity.

IV. CONCLUSION

NIADA would like to thank the Agencies and the FTC for the opportunity to comment with respect to the requirements under the Red Flag 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, LLC located at 6300 Frantz Road, Dublin, Ohio 43017.

[11] 2006 NIADA Independent Used Car Industry Report, National Independent Automobile Dealers Association, 2521 Brown Blvd., Arlington, TX 76006, and Leedom, and Associates, LLC, 40 Sarasota Center Blvd., Suite E, Sarasota, FL 34277.